



11/19/99

ATTORNEY DOCKET NO. 5442-020

BOX NEW APP  
 THE ASSISTANT COMMISSIONER FOR PATENTS  
 WASHINGTON, D.C. 20231

SIR:

TRANSMITTED HEREWITH FOR FILING IS THE PATENT APPLICATION OF

INVENTOR(S): LUC VANTALON, ET AL.

FOR: DIGITAL TELEVISION CONDITIONAL ACCESS METHODS AND APPARATUS WITH MULTIPLE DATA TRANSPORT MECHANISM

ENCLOSED ARE:

28 PAGES SPECIFICATION, 42 CLAIMS (13 pgs), 21 SHEETS OF FORMAL DRAWINGS, AND 1 PAGE ABSTRACT.

1 PAGE INVENTOR LIST.

A VERIFIED STATEMENT TO ESTABLISH SMALL ENTITY STATUS UNDER 37 CFR 1.9(f) and 1.27 (b)

ALSO ENCLOSED: DECLARATION AND POWER OF ATTORNEY (UNSIGNED)

THE FILING FEE IS CALCULATED BELOW

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	42-20 =	22	X \$ 18 =	\$ 396.00
	INDEPENDENT	12- 3 =	9	X \$ 78 =	\$ 702.00
	MULTIPLE DEPENDENT CLAIMS (if applicable)			+ \$260 =	\$ 0
	LATE FILING OF DECLARATION			+ \$130 =	\$ 0
				BASIC FEE	\$ 760.00
				TOTAL OF ABOVE CALCULATIONS =	\$1,858.00
	Reduction by 50% for filing by Small Entity				0
	<input type="checkbox"/> RECORDATION OF ASSIGNMENT			+ \$ 40 =	\$ 0
				TOTAL	\$1,858.00

In view of the Unsigned Declaration as filed with this application and pursuant to 37 CFR 1.53(f), Applicants request deferral of the filing fee until submission of the Missing Parts of Application.

SABATH &amp; TRUONG

Robert P. Sabath  
 Attorney of Applicant  
 Reg. No. 29,107

111 N. Market Street  
 Suite 815  
 San Jose, California 95113  
 Tel: (408) 293-9934  
 Fax: (408) 293-2183

"Express Mail" mailing number E334603989US  
 Date of Deposit November 19, 1999

I hereby certify that this paper or fee is being deposited with the United States Postal Service, Express Mail Post Office to Addressee service, under 37 CFR 1.10 on the date indicated above and is addressed to Box NEW APP, Assistant Commissioner for Patents, Washington, D.C. 20231.

Annette Jacobs  
 Name

November 19, 1999  
 Date

jc625 U.S. PTO  
 09/444486  
 11/19/99



**DIGITAL TELEVISION CONDITIONAL ACCESS METHODS AND  
APPARATUS WITH MULTIPLE DATA TRANSPORT MECHANISM**

**INVENTOR(S):** Luc Vantalon  
a citizen of France  
residing at  
1396 Cordilleras Avenue  
Sunnyvale, California 94087

Arnaud Chataignier  
a citizen of France  
residing at  
31 allée de la Granette  
F-13600 Ceyreste  
France

Christophe Genevois  
a citizen of France  
residing at  
47, Avenue de la Paix  
13600 La Ciotat  
France

**Assignee:** SCM Microsystems (U.S.), Inc.  
160 Knowles Drive  
Los Gatos, California 95032

**Entity Status:** Large

## PATENT APPLICATION

### **DIGITAL TELEVISION CONDITIONAL ACCESS METHODS AND APPARATUS WITH MULTIPLE DATA TRANSPORT MECHANISM**

5

#### DESCRIPTION

#### **CROSS-REFERENCE TO RELATED APPLICATIONS**

This application is related to the following copending patent applications:

10 (1) Serial No. (Docket 5442-021) , filed on even date herewith, entitled "Adaptive Trans-Scrambling Mechanism for Digital Television Multiple Data Transport System" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois ; (2) Serial No. (Docket 5442-022) , filed on even date herewith, entitled "Digital Television Methods and Apparatus" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois; and (3) Serial No. (Docket 5442-023) , filed on even date herewith, entitled "Signal Filtering Mechanism for a Multi-Purpose Digital Television Receiver" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois. The foregoing cross-referenced patent applications are expressly incorporated in their entirety into this application by this reference thereto.

#### **TECHNICAL FIELD**

This invention relates to digital television systems and services and particularly to conditional access methods and apparatus for use with such systems and services.

## **BACKGROUND OF THE INVENTION**

Digital television is an emerging technology which is becoming increasingly popular with the public. One of the more interesting aspects is the introduction of so-called "high-definition television" (HDTV), the broadcasting of which was recently 5 approved by the United States Federal Communications Commission. HDTV will provide television images of much higher quality and definition than is provided by preexisting "conventional definition" television systems.

Another highly important aspect of digital television is the providing of related services, such as video-on-demand programming, pay-per-view movies and sporting 10 events, interactive video games, home shopping capabilities, high-speed Internet access and the like. The home television set is fast becoming the predominate 15 information and services dispensing medium of the future.

As is known, television services are presently communicated by land-based 20 radio-type broadcast transmissions, cable network transmissions and space satellite transmissions. In order to limit reception to paid subscribers, it is common practice for cable and satellite providers to scramble their transmissions and to require their customers to use a special set-top control box to unscramble the received signals. Such scrambling and set-top box techniques are also desired by providers of related services. The problem to date is that each provider has developed its own unique and 25 proprietary set-top control box. Thus, to receive and use signals from multiple

providers requires the use of multiple set-top control boxes. This is not the best situation and, in order to overcome the problem, the U. S. Federal Communications Commission is encouraging a so-called "open" receiver approach for providing a universal set-top box capable of receiving and handling content from multiple providers. Unfortunately, this is not an easy thing to do and at the same time provide the security control features needed to protect the various service providers from loss of services to unauthorized users.

## **SUMMARY OF THE INVENTION**

The present invention provides an efficient and flexible security mechanism for use with a "universal" set-top control box. This security mechanism grants conditional access to the transmitted program material in a manner, which provides a high degree of protection against unauthorized use of the material. This conditional access mechanism includes a multi-transport capability, which performs descrambling and filtering operations on different transmission protocols by qualifying the different components of the transport layer using a unique coding technique.

The multiple transport apparatus of the present invention is capable of automatically handling several different data transport stream formats. It can, for example, handle MPEG, DSS and ATM type data transport streams. This is accomplished by qualifying each newly-received data byte according to its position

and value within its packet. A plural-bit tag is assigned to each data byte, such tag having a value determined by the qualifying process. The qualified and tagged data byte provides all the information required for further processing of the data byte. The qualification mechanism is unique and is not dependent on the transport system used for carrying the received packet bytes. The qualification mechanism supports both broadcast and burst transmission modes and it provides all the information required for further processing.

For a better understanding of the present invention, together with other and further advantages and features thereof, reference is made to the following description taken in connection with the accompanying drawings, the scope of the invention being pointed out in the appended claims.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

Referring to the drawings:

15 FIG. 1 is a general block diagram of a digital television receiving system with a security mechanism for preventing unauthorized display of the transmitted images; FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1; FIG. 3 is a conceptual diagram for one embodiment of the present invention; FIG. 4 shows in greater detail a representative form of internal construction for 20 the set-top box and the conditional access module of FIG. 2B;

FIG. 5 is a detailed block diagram for the transport stream co-processor and the microprocessor unit of the conditional access module of FIG. 4;

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention;

5 FIG. 7 shows a representative form of construction for a microprocessor-to-microprocessor data channel feature of the present invention;

FIG. 8 shows a representative form of construction for a Smart Card channel feature of the present invention;

40 FIG. 9 shows representative form of construction for the transport stream (TS) input unit of FIG. 5;

FIG. 10 shows in more detail a representative form of construction for the cipher bank unit of FIG. 5;

FIG. 11 shows a general form of construction for the cipher processor of FIG. 10;

15 FIG. 12 shows the details of a representative form of construction for the conditional access descrambler of FIG. 11;

FIG. 13 shows the details of a representative form of construction for the copy protect scrambler of FIG. 11;

FIG. 14 shows a representative form of construction for the filter bank unit of

20 FIG. 5;

FIG. 15 shows in greater detail the construction of one of the filter units of FIG. 14;

FIG. 16 is a plan view of one form of PCMCIA Smart Card reader that may be used with the present invention;

5 FIG. 16A is a left end view of the FIG. 16 card reader;

FIG. 16B is a right end view of the FIG. 16 card reader;

FIG. 16C is a side view showing one side of the card reader of FIG. 16;

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention;

40 FIG. 18 shows a further form of card reader that may be used;

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention;

FIG. 22 is a flow chart used in explaining a multiple data transport feature of the present invention; and

15 FIG. 23 is a detailed flow chart for a representative implementation of the method of FIG. 22.

## **DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS**

Referring to FIG. 1, there is shown a general block diagram of a digital

20 broadband receiving system having one or more receivers 10 connected to one or

more broadband signal transmission networks. Typical signal transmission networks include land-based radio-frequency type broadcast networks, cable networks, space satellite signal transmission networks, broadband telephone networks, etc. The analog information signals intended for transmission (for example: video signals, audio

5 signals, or data signals) are converted to specific digital transport stream formats for transmission purposes. Typical transport stream formats are the MPEG format, the DSS format and the ATM format. The MPEG format is the data transmission format developed by the Motion Picture Expert Group. A preferred form of MPEG is MPEG-2, which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals used by some satellite operators. The acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal protocol for efficient transport of both fixed rate and bursty information in broadband digital networks. The ATM digital stream consists of fixed length packets called "cells."

15 Each receiver 10 demodulates its received signal and supplies the demodulated signal to a security mechanism 11. Security mechanism 11 selects one or more of the received signal transport streams and removes the network distribution security layers therefrom, provided the end user is entitled to receive the signals. Network security mechanism 11 also applies content protection to any of the signal streams that require 20 it. The resulting signals are supplied to decoders 12 which select one or more of the

signal streams and decodes each selected stream to recreate the desired video, audio and data signals which are, in turn, supplied to one or more display units 13 and one or more recording units 14. Typical display units include television sets and television and computer monitors. Typical recording units include VCR-type video recorders and various types of computer memory units. Security mechanism 11 examines the received signal or signals and determines their types and controls their descrambling. Security mechanism 11 allows access to an unscrambled version of the received signal, provided the required conditions are met.

In addition to regular digital television programming, the receiving system of FIG. 1 also receives and handles various related communications services. Examples of related services are video-on-demand programming, pay-per-view movies and sporting events, interactive video games, home shopping services, high-speed Internet access, and the like. As will be seen, the data signals and control signals for these related services over a two-way cable system are supplied by way of a so-called "out-of-band" channel.

FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1. In particular, FIG. 2A shows the case where the receivers 10, security mechanism 11 and decoders 12 are located within a network specific set-top box 15. In one case, the security mechanism 11 is imbedded within or permanently mounted within the set-top box 15. In a typical use, the set-top box 15 sits on top of the display unit 13.

FIG. 2B shows an open-type set-top box 16 with a renewable and removable add-on security mechanism represented by a conditional access module (CAM) 17. Conditional access module 17 performs the security functions provided by the security mechanism 11 of FIG. 2A. Conditional access module 17 is a removable plug-in type element which is adapted to be plugged into a cooperating receptacle or socket in the host set-top box 16. As in FIG. 2A, set-top box 16 is designed to sit on top of the display unit 13.

FIG. 2C shows the case where the set-top box functions are located inside the cabinet 18 of a television receiver, that is, the cabinet which houses the display unit or picture tube 13. The conditional access module 17 is adapted to plug into a cooperative receptacle which is accessible from the outside of the cabinet 18. FIG. 2C represents an integrated television set with a renewable, add-on security mechanism represented by the conditional access module 17.

FIG. 2D represents the case where the primary units are located in separate component-type cabinets or boxes 19a-19d. The conditional access module 17 may be removably plugged into the receiver box 19a or the decoder box 19b or may, instead, be part of a small connector unit which is connected between boxes 19a and 19b. The configuration of FIG. 2D would be particularly useful in a component-type entertainment center intended for home use.

Referring to FIG. 3, there is shown a conceptual diagram for one embodiment

of the present invention. As there seen, the receiving apparatus includes an in-band channel 20 and an out-of-band channel 21, which are adapted to receive incoming signals from a cable system head-end. The in-band channel 20 handles the primary user signals, such as the digital television signals. The out-of-band channel 21 handles the digital control signals for the related services, such as video-on-demand commands, security data, e-commerce transactions, etc. Both of channels 20 and 21 communicate with various application programs 22 by way of a filter bank 23 which detects various defined digital patterns within the received signals and reacts thereto for establishing connections with the appropriate ones of applications 22.

The apparatus of FIG. 3 also includes a smart card channel 24 for providing communications between a smart card SC and the applications programs 22. A data channel 25 provides communications between a CPU (Central Processing Unit) located in the host unit, for example, set-top box (STB) 16, and the application programs 22. An extended channel 26 is provided to transfer network data over the out-of-band channel from the network to the host CPU or vice versa.

Referring to FIG. 4 there is shown in greater detail a representative form of internal instruction for the host unit or set-top box 16 and the conditional access module 17 of FIG. 2B. As seen in FIG. 4, a signal connector 29 connects the set-top box 16 to the communications network supplying the signals. This signal path 29 runs to an in-band receiver 30 and an out-of-band receiver 31. The communications

network is a multi-channel system and the channel conveying the primary video and audio signals is labeled as the "in-band" channel and the channel which carries the control signals for the related services is called the "out-of-band" channel. The set-top box 16 further includes an out-of-band transmitter 32 for transmitting signals back to the digital data provider located at the network broadcasting center.

5 The digital signals appearing at the outputs of receivers 30 and 31 are supplied to the conditional access module 17. The primary video and audio signals are supplied back to a decoder 33 in the set-top box 16 and from there to the digital TV display 13. The set-top box 16 includes a microprocessor unit 34, which, among other things, provides control signals to the decoder 33. A memory unit 36 is coupled to the microprocessor unit 34 and, among other things, provides storage for various control routines and application program functions utilized by the microprocessor unit 34. Microprocessor unit 34 and memory 36 provide a CPU function for the set-top box 16.

10 The conditional access module (CAM) 17 of FIG. 4 includes a transport stream (TS) co-processor 40 which receives the output digital signals from the in-band receiver 30 and the out-of-band receiver 31, the latter being supplied by way of an out-of-band decoder 41. Transport stream co-processor 40 also supplies the digital video and digital audio signals, which are intended for the TV display 13, to the decoder 33.

15 Conditional access module 17 further includes a microprocessor unit 42 and an associated memory unit 43. These units 42 and 43 provide a CPU function for the

conditional access module 17. The primary portion of the application programs 22 are stored in the memory 43. A data channel 44 provides a direct communications link between the CAM microprocessor unit 42 and the host microprocessor unit 34. The CAM microprocessor unit 42 can also send digital messages and information back to the cable head-end. This is done by way of an out-of-band encoder 45 and the out-of-band transmitter 32 in the host set-top box 16. A removable smart card 28 is adapted to be connected to the microprocessor unit 42 for supplying control information thereto.

An extended channel is provided for enabling the cable head-end to communicate with the host microprocessor unit 34 and vice-versa. The incoming branch of this extended channel includes a signal path 47 coupled to the out-of-band receiver 31 and extending to the out-of-band decoder 41. This incoming branch includes the decoder 41, transport stream co-processor 40, microprocessor 42 and a further signal path 49 which runs from the microprocessor 42 to the host microprocessor 34. The outgoing branch of this extended channel is provided by a signal path 50 which runs from the host microprocessor 34 directly to the out-of-band encoder 45.

Referring to FIG. 5, there is shown a detailed block diagram for the transport stream (TS) co-processor 40 and the microprocessor unit 42 of the conditional access module (CAM) 17 of FIG. 4. As seen in FIG. 5, the transport stream (TS) co-

processor 40 includes a transport stream (TS) input unit 52 which receives parallel-type digital input signals TSin1 and TSin2 from the in-band receiver 30 and the out-of-band receiver 31, respectively. An additional serial-type digital signal input TSin3 is added for processing other signals. The output signals from the input unit 52 are 5 supplied to a cipher bank 54 for further processing. Cipher bank 54 produces two parallel type output streams which are connected to the inputs of a TS output unit 55 and a filter bank 56. By multiplexer selection within the cipher bank 54, one of the two input streams to the cipher bank 54 is processed by an internal cipher processor, while the other input stream is simply bypassed to the TS output unit 55 and the filter bank 56. The TSout signal from TS output unit 55 is supplied to the decoder 33 in the set-top box 16 .

The transport stream input unit 52 includes a multiple data transport mechanism capable of receiving a plurality of different transport stream formats. In particular, it includes a qualifying mechanism for receiving and qualifying incoming 15 data bytes according to their positions and values in their plural-byte data packets. TS input unit 52 further includes a tagging mechanism for assigning a plural-bit tag to each data byte, such tag having a unique value determined by the results of the qualifying process. The tag bits are used to facilitate the further processing of the data bytes.

20 The microprocessor unit 42 includes a microprocessor 60 which is connected to

a 32-bit system bus ASB which typically operates in a high speed transfer mode. Also connected to the ASB bus are a memory interface unit 61, an address decoder unit 62, an arbiter unit 63, and a read only memory (ROM) unit 64. Memory interface 61 is connected to the external memory 43 associated with the microprocessor unit 42.

5 The microprocessor 60 communicates with the transport stream coprocessor 40 and various other units by means of a peripheral bus VPB. This VPB bus is connected to the microprocessor 60 by way of a bus-to-bus bridge unit 65 and the high- speed ASB bus. The ASB bus is used for fast transfers and the VPB bus is used for communications with a lower priority. As the filter bank 56 of co-processor 40 needs a direct and fast access to the external memory 43 for its output data, it is also connected to the ASB bus. As a consequence, there are three masters on the ABS bus, namely, the microprocessor 60 and the two channels of the filter bank 56. The arbitration between these masters is managed by the arbiter unit 63. By way of comparison, the VPB bus has only a single master, namely, the microprocessor 60.

15 The address decoder 62 decodes the address bits on the ASB bus to select the right target for the data on the ASB bus. Typical targets are the memory interface 61, ROM 64 and the various peripherals and other units connected to the ASB bus. An interrupt controller 66 provides the interrupt function for the microprocessor 60, while a timer 67 provides various timing functions. Each of the units in the transport stream 20 co-processor 40 is coupled to the lower priority VPB bus for control and status

purposes. Also coupled to the VPB bus are an extended channel unit 68, a data channel unit 69 and a PCMCIA interface 70. A peripheral interface unit 71 provides an interface between the VPB bus and one or more peripheral devices. For example, a smart card interface connector structure 72 is provided for making connection with a removable smart card 28 shown in FIG. 4. A serial interface 73 may be provided for connecting to a serial type peripheral device PD.

5

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention. This out-of-band channel feature includes an out-of-band channel decoder 41 which receives the out-of-band signal OBin from the out-of-band receiver 31 shown in FIG. 4. The output of decoder 41 is supplied by way of the transport stream co-processor 40 for further filtering operations. The outgoing or transmitter portion of the out-of-band channel includes ATM encoder 48, transmit buffer 46 and a channel encoder 45 which supplies the out-of-band output signal OBout to the out-of-band transmitter 32 shown in FIG. 4. The ATM encoder 48 receives its input signal from the VPB peripheral bus associated with the microprocessor unit 42. The data to be transmitted is supplied by either the application programs located in the microprocessor unit 42 or the data received from the set-top box 16 by way of the extended channel path 50. This data is segmented into ATM cells by the ATM encoder 48. These cells are temporarily stored in the buffer 46. When the network grants some transmission slots to the conditional access

10

15

20

module 17, the transmit buffer 46 is emptied by channel encoder 45 and is transmitted by way of out-of-band transmitter 32 to the cable head-end.

FIG. 7 shows a microprocessor-to-microprocessor data channel feature of the present invention. This feature enables the CAM microprocessor unit 42 to communicate directly with the host microprocessor unit 34 and vice-versa.

Microprocessor unit 42 sends data to the microprocessor unit 34 by way of data channel 44a. The host unit 34 sends data to the CAM microprocessor 42 by way of data channel 44b.

FIG. 8 shows the details of the smart card (SC) interface 72 of FIG. 5. The smart card 28 is adapted to be inserted into a smart card reader 86 and the data received from the smart card 28 is supplied by way of an input buffer 87 to the peripheral bus VPB associated with the microprocessor unit 42. Data from the microprocessor unit 42 is supplied by way of the VPB bus, output buffer 88 and the smart card reader 86 to the smart card 28. In a representative embodiment, smart card reader 86 is a PCMCIA card reader. The acronym PCMCIA stands for Personal Computer Memory Card International Association. This is a non-profit trade association founded in 1989 to define a standard memory card interface. The smart card reader 86 complies with this interface standard.

Referring now to FIG. 9 there is shown in greater detail a representative form of construction for the transport stream input unit 52 of FIG. 5. The TSin1 and TSin2

5

signals are supplied to input registers 130 and 131. The serial input signal TSin3 is supplied to a serial-to-parallel converter 132 which converts same from serial form to parallel form. The parallel output of converter 132 is supplied to a further input register 133. The outputs of registers 130, 131, and 133 are connected to a three-to-  
two multiplexer 134. This multiplexer 134 selects two out of the three inputs and supplies one of the selected inputs to a TS1 FIFO unit 135 and the other of the selected inputs to a TS2 counter unit 136. FIFO 135 provides the input for a TS1 parser 137, while the counter 136 provides the input for a TS2 parser 138. Parsers 137 and 138 analyze their respective signal streams on a byte-by-byte basis and assign a plural-bit tag to each data byte. More particularly, each of parsers 137 and 138 includes a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets. In a representative embodiment, a 5-bit tag is generated for and attached to each data byte. The value of this 5-bit tag is determined by the qualifying process performed by the  
15 qualifying mechanism. Parsers 137 and 138 are, in turn, connected to a selection parser 139 which determines the particular output path, TSa or TSb, to which each data stream is connected.

15

20

Referring to FIG. 10, there is shown in more detail a representative form of construction for the cipher bank 54 of FIG. 5. Cipher bank 54 receives the two signal streams TSa and TSb from the TS input unit 52 of FIG. 9. The two output buses 74

and 75 from cipher bank 54 are connected to the TS output unit 55 and the filter bank 56. Thus, the cipher bank 54 has two input streams and two output streams. By selection via multiplexers 76, 77, and 78, one of the input streams is processed by a cipher processor 79, while the other input stream is simply bypassed to the output of 5 its corresponding one of multiplexers 77 and 78. Multiplexers 76, 77 and 78 are controlled by selection signals S1, S2 and S3, respectively, obtained by way of the VPB bus.

For a first set of multiplexer settings, the TSa data stream is transferred by way of multiplexer 76 to the cipher processor 79 and the output of cipher processor 79 is transferred by way of multiplexer 77 to the TSout1 bus 74 of the cipher bank 54. For this same case, the second input data stream TSb, is supplied by way of multiplexer 78 to the TSout2 bus 75. For the second set of multiplexer settings, the situation is reversed. The TSb data stream is supplied by way of multiplexer 76 to the cipher processor 79 and the resulting processed signal is supplied by way of multiplexer 78 to 15 the TSout2 bus 75. In this second case, the TSa input data stream is supplied by way of multiplexer 77 to the TSout1 bus 74. Cipher processor 79 outputs both a protected data stream TSp and a clear data stream TSc. Multiplexers 77 and 78 select one or the other, but not both of these data streams.

Referring to FIG. 11, there is shown the primary elements of the cipher 20 processor 79 of FIG. 10. As seen in FIG. 11, cipher processor 79 includes a

conditional access descrambler 80 and a copy protection scrambler 81. Descrambler 80 removes the network scrambling protection layer. Descrambler 80 is capable of descrambling the following encryption formats: the DVB super scrambling format used in Europe, the DES and 3DES data encryption standard formats which are used in the United States, and the MULTI2 format which is used in Japan. The copy protect scrambler 81 adds a content scrambling protection layer to the clear copy signal at the output of descrambler 80 to preclude the data content from being stolen at the output of the conditional access module 17 this being particularly significant when it is copyrighted material. Scrambler 81 uses the DES data encryption standard scrambling method.

Cipher processor 79 is an adaptive trans-scrambler for converting one encryption format to a different encryption format. This enables the conditional access module 17 to accommodate a relatively large number of different incoming encryption formats.

FIG. 12 shows the details of a representative form of construction for the conditional access descrambler 80 of FIG. 11. The descrambler 80 of FIG. 12 includes an input data register 140 for receiving the TSin data stream from the multiplexer 76 of FIG. 10. Descrambler 80 also includes a set of four cryptographic engines 141-144 that share the same control logic and key registers for descrambling any one of the following encryption formats: DVB, DES, MULTI2 and 3DES. The

DES and 3DES cryptographic engines 142 and 144 include programmable feedback registers to support most of the DES modes of operation as defined by the Federal Information Processing Standards Publication (FIPS) PUB81 namely, the DES-ECB, DES-CBC, DES-OFB, 3DES-ECB, 3DES-CBC and 3DES-OFB modes. Other 5 encryption formats can be accommodated by providing appropriate additional cryptographic engines. The foregoing acronyms have the following meanings:

<u>ACRONYM</u>	<u>DESCRIPTION</u>
DVB	Digital Video Broadcasting (Europe)
DES	Data Encryption Standard (U.S.)
ECB	Electronic Code Book
CBC	Cipher Block Chaining
OFB	Output Feedback

A descramble format register 150 and an associated decoder 151 determine which one of the primary cryptographic engines 141-144 is activated to process the incoming data stream. Descramble format register 150 is loaded by way of the VPB bus with a plural-bit control signal which designates the cryptographic engine to be used. This control signal combined with an analysis of the position of the data byte 20 within its transport packet defines which feedback mode of operation is applied for a given data byte. Thus, only a selected one of the cryptographic engines 141-145 is activated for any given transport stream and one feedback mode of operation is used for any given data byte within the transport stream.

The active session key pairs in session key register 152 are uniquely renewed whatever the active cryptographic engine and the feedback mode of operation. When 3DES engine 144 is the active cryptographic engine, three times less key pairs are stored in session key register 152. The data register 140 selects which key pair is 5 valid for a given data byte, depending on to which transport packet it belongs. Then descrambling key pairs are loaded into session key register 152 by way of The VPB bus. Register 152, in turn, supplies the descrambling key pair to the active one of cryptographic engine 141-144. The descrambled data stream appearing at the output of the selected one of cryptographic engines 141-144 is supplied to an output data register 153 to provide a clear or unscrambled output signal TSclear or TSc.

10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95

Referring now to FIG. 13, there is shown the details of a representative form of construction for the copy protect scrambler 81 of FIG. 11. For the embodiment shown in FIG. 13, The descrambler 81 includes a DES encryption engine 154 and supports most of the DES modes of operation as defined by the Federal Information Processing 15 Standards Publication PUB 81 these modes are represented by DES-ECB, DES-CBC and DES-OFB encoders 155-157. Selection of a desired mode of operation is accomplished by means of a plural-bit control signal which is loaded into a scramble format register 158. This control signal controls an enable decoder 159 to activate a select one of its output lines, which output lines individually run to different ones of 20 the encoders 155-157. The scrambled data stream appearing at the output of the

selected encoder is supplied to an output data register 160 to provide the copy protected output signal TSprotected or TSp. The actual scrambling process which is followed in the selected encoder is controlled by a plural-bit scrambling session key which is loaded into a session key register 161. This scrambling session key is

5 obtained from the microprocessor unit 42 by way of The VPB bus.

Referring now to FIG. 14, there is shown a representative form of construction for the filter bank 56 of FIG. 5. This filter bank 56 examines incoming data streams to determine the type of data packets being received. When a desired packet is identified, its data payload is then stored in the proper location in memory 43 which is assigned to its particular packet type. In this way, the incoming data may be filtered or sorted according to the application or use for which it is intended. Filter bank 56 has two inputs FLTin1 and FLTin2 which are received from cipher bank 54. These inputs may convey different transport stream formats.

The filter bank 56 includes four filter units 90-93 which can be independently set up to process different data streams. This architecture allows a flexible adjustment of the filtering resources depending on the type of application. For example, if the 15 conditional access module is set up to support ATSC-type advanced television services (for example, high-definition television), the four filter units 90-93 are tuned to the in-band channel. For an open cable type of operation, on the other hand, up to three of the filter units can be set to process the out-of-band channel for collecting IP

20

and proprietary messages, while the fourth filter unit must stay tuned to the in-band channel for processing in-band command signals. The outputs of filter units 90-93 are selectively connected to the microprocessor ASB bus by a multiplexer 94 which is controlled by switching signal S4.

5 FIG. 15 shows in greater detail a representative form of construction for one of the filter units 90-93 of FIG. 11. Each of the filter units 90-93 is of this same construction. The filter unit of FIG. 15 is tuned to one of the two inputs FLTin1 and FLTin2 by a multiplexer 95 which is set to select one of the two inputs by a selector signal S5. The selected input data stream is supplied to a Type Filter 96 which prefilters the data bytes according to the plural-bit tags attached to them in the TS input unit 52 of FIG. 9. The pre-filtered bytes are then sent to an array of filter cells 97a-97h for further value comparison. Pre-recorded signal patterns which it is desired to detect are stored in a pattern memory 98 and are supplied to filter cells 97a-97h.

10 When a pattern match occurs, the corresponding filter cell loads a shift register 99. Complete messages are extracted from shift register 99 for storage in the memory unit 43 associated with the CAM microprocessor unit 42.

15 FIG. 16 is a plan view of one form of PCMCIA smart card reader that may be used with the present invention. FIG. 16A is a left-end view, FIG. 16B is a right-end view and FIG. 16C is a side view of the card reader shown in FIG. 16. The acronym 20 PCMCIA stands for Personal Computer Memory Card International Association. This

is a non-profit trade association formed in 1989 to define a standard memory card interface. The smart card reader of FIG. 16 includes a metallic casing 100 which is adapted to receive a plastic memory card or smart card of approximately the size of a plastic credit card. The casing 100 conforms to ISO Standard 7816. In use, the smart 5 card is inserted into the casing 100 and the casing 100 is, in turn, inserted into an appropriate connector receptacle in the set-top-box 16.

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention. The reader casing 101 of FIG. 17 has a shorter extension, hence, a shorter overall length. FIG. 18 shows a further form of card reader 10 that may be used. The reader casing 102 of FIG. 18 is a so-called dual reader casing and is adapted to receive two different smart cards.

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention. FIG. 19 shows the format for an MPEG data stream packet. FIG. 20 shows the format for a DSS data stream packet and FIG. 21 shows the format for an ATM data stream cell. The MPEG format is the data transmission format developed by the Motion Picture Expert Group. The preferred form of MPEG is MPEG-2 which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals by some satellite operators. The 15 acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal 20 format.

5

protocol for efficient transport of both constant rate and burst type information in broadband digital networks. The ATM digital stream consists of fixed-length packets called "cells". Each cell contains 53 8-bit bytes and is comprised of a 5-byte header and a 48-byte information payload. The digital television signal standard approved for use in the United States employs The MPEG-2 transport stream format for packeting and multiplexing the video, audio and data signals.

10

An MPEG packet has an overall length of 188 bytes and includes a 4-byte header field and a variable length adaptation field which can vary in length from zero bytes to several bytes. The remainder of the packet is comprised of payload bytes. A DSS packet has an overall length of 130 bytes and includes a 3-byte header field and an optional variable length adaptation field of relatively-small length. The remainder of the DSS packet is comprised of payload bytes.

15

20

FIG. 22 is a flow chart which explains the general nature of the multiple data transport feature of the present invention. Each newly received data byte (block 103) is examined and qualified according to its position and value in its data packet (block 125). The examined byte is then tagged with a plural-bit tag (block 126), the value of the tag being determined by the results of the qualifying process (block 125). The resulting tagged byte is then passed on as a qualified byte (block 124). In the present embodiment, the process described by FIG. 22 is performed by the TS input unit 52 shown in FIG. 9. The qualification and tagging of The received data bytes is

performed by The parsers 137 and 138.

Referring to FIG. 23, there is shown a detailed flow chart for a representative implementation of The method of FIG. 22. This multiple transport method of FIG. 23 enables The conditional access module 17 to handle any of The MPEG, ATM and DSS transport stream formats. Each incoming data byte is qualified according to its position and value within its packet. This qualification mechanism attaches a 5-bit tag to each data byte, which tag contains all The information required for further processing of The byte. The qualification of each new byte starts with block 103 of FIG. 23, which block represents The reception of The new byte. The byte is first examined to determine if it is a header byte (block 104). If it is, a determination is then made as to whether it contains channel identification (ID) data (block 105). If The answer is yes, The byte is assigned a 3-bit tag portion having a value of "011" (block 106). If it is not a channel ID, then The byte is assigned a 3-bit tag portion having a value of "010" (block 107). Note that The total tag is a 5-bit tag. The purpose of The other two bits will be described shortly.

If The determination of block 104 determines that The new byte is not a header byte, then The byte undergoes a series of further non-header byte tests. The first test, represented by block 108, is to determine whether The byte is a null byte. If yes, it is assigned a 3-bit tag having a code of "000", as indicated by block 109. If The answer is no, then The byte proceeds to an adaptation field test represented by block 110. If

The byte is an adaptation field byte, then it is assigned a tag value of "101", as represented by block 111. If it is not an adaptation field byte, then The test of block 112 is performed to determine whether or not it is a table identification (ID) byte. If yes, The byte is assigned a 3-bit tag having a value of "110", as represented by block 113. If no, The byte is examined per block 114 to determined whether it is a section length indicator byte. If yes, it is assigned a 3-bit tag value of "001", as indicated at block 115. If no, The byte proceeds to The payload decision block 116. Since this is The only alternative left, The byte is determined to be a payload byte and is given a 3-bit tag portion having a value of "111", as indicated at block 117.

10 After assignment of The initial 3-bit portion of its tag, The newly received byte is tested as indicated by decision block 118, to determine whether its data is scrambled or clear. If scrambled, a fourth bit in The tag, namely, The SCR bit is set to 1. If not scrambled, The SCR bit is set to 0. The byte is then tested as indicated by block 121 to determine whether it is The last byte of either a header field or a payload field. If it 15 is a last byte, The LTB bit (The fifth bit in The 5-bit tag) is set to 1 (block 122) and if not, The LTB bit is set to 0 (block 123). This completes The qualification process and The qualified output byte at step 124 is now in condition for further processing in The conditional access module 17.

20 The qualification process of FIG. 23 produces a stream of output bytes which are no longer dependent on The particular transport stream format which brought them

to The conditional access module 17. Thus, The conditional access module 17 is enabled to process a variety of different transport stream formats in an efficient manner with minimal complication. And while the described implementation supports The MPEG, DSS and ATM transport stream formats, it can be readily extended to handle other packet-type or cell-type transport structures.

5 While there have been described what are at present considered to be preferred embodiments of this invention, it will be obvious to those skilled in the art that various changes and modifications may be made therein without departing from the invention and it is, therefore, intended to cover all such changes and modifications coming 10 within the true spirit and scope of the invention.

## CLAIMS

What is claimed is:

1        1. A multiple data transport method for enabling a conditional access module

2        to handle any of a plurality of data transport stream formats, said multiple transport

3        method comprising:

4                qualifying received data bytes according to their positions and values within a

5                data packet; and

6                attaching a multi-bit tag to each received data byte, such tag containing

7                information required for further processing of the byte.

1        2. The multiple transport method according to claim 1 further comprising

2        examining each byte to determine if it is a header byte.

1        3. The multiple transport method according to claim 2 further comprising

2        determining whether the byte contains channel identification data.

1        4. The multiple transport method according to claim 3, including performing

2        an adaptation field test.

1           5. The multiple transport method according to claim 4 including determining  
2           whether the byte is a payload byte.

1           6. The multiple transport method according to claim 5 including determining  
2           whether the data in the byte is scrambled or clear.

1           7. The multiple transport method according to claim 1 including producing a  
2           stream of output bytes which are no longer dependent on the particular transport  
3           stream format in which they arrived at the conditional access module.

1           8. A multiple data transport system for enabling a conditional access module to  
2           handle any of a plurality of data transport stream formats, said multiple transport  
3           system comprising:

4           a qualification mechanism for qualifying received data bytes according to their  
5           positions and values within a data packet; and  
6           a tagging mechanism for applying a multi-bit tag to each received data byte,  
7           such tag containing information required for further processing of the byte.

1           9. The multiple transport method according to claim 8 including a mechanism  
2           for examining each byte to determine if it is a header byte.

1           10. The multiple transport system according to claim 9 further comprising a  
2           mechanism for determining whether the byte contains channel identification data.

1           11. The multiple transport system according to claim 10 including performing  
2           an adaptation field test.

1           12. The multiple transport system according to claim 11 including a  
2           mechanism for determining whether the byte is a payload byte.

1           13. The multiple transport system according to claim 12 including a  
2           mechanism for determining whether the data in the byte is scrambled or clear.

1           14. The multiple transport system according to claim 8 including a mechanism  
2           producing a stream of output bytes which are not dependent on the particular transport  
3           stream format in which they arrived at the conditional access module.

1           15. The multiple transport system according to claim 8 configured to receive  
2           input transport streams formatted according to MPEG, DSS and ATM transport stream  
3           formats.

1           16. The multiple transport system according to claim 8 configured to receive  
2           packet-type and cell-type transport structures.

1           17. A multiple data transport mechanism capable of receiving a plurality of  
2           different transport stream formats, such mechanism comprising:

3           a qualifying mechanism for receiving and qualifying incoming data bytes  
4           according to their positions and values in their plural-byte data packets; and  
5           a tagging mechanism for assigning a plural-bit tag to each data byte, such tag  
6           having a value determined by the results of the qualifying process performed by the  
7           qualifying mechanism.

1           18. A method for handling any of a plurality of transport stream formats, said  
2           method comprising:

3           qualifying received data bytes according to their positions and values; and  
4           attaching a tag to each qualified data byte.

1           19. A digital broadband receiving system comprising:

2           a plurality of receivers configured for communication with one or more

3 broadband signal transmission sources producing signals in a transport stream format  
4 such as, for example, MPEG format, DSS format, or ATM format; and  
5 a security mechanism connected to each of said plurality of receivers, said  
6 security mechanism configured to select one or more of the received signal transport  
7 streams and to remove the network distribution security layers therefrom.

1  
2 20. The digital broadband receiving system according to claim 19, wherein  
3 said network security mechanism applies content protection to any of the signal  
4 streams that require it.

1  
2 21. The digital broadband receiving system according to claim 19 further  
3 including a plurality of decoders which are configured to select one or more of the  
4 signal streams and to decode each selected stream to recreate desired video, audio and  
5 data signals which are, in turn, supplied to one or more display units or one or more  
recording units.

1  
2 22. The digital broadband receiving system according to claim 19 wherein said  
3 security mechanism is configured to examine received signals to determine their types.

1  
2 23. The digital broadband receiving system according to claim 22 wherein said

2 security mechanism is configured to control descrambling of received signals.

1 24. A set-top system comprising:

2 a plurality of receivers configured for communication with one or more

3 broadband signal transmission sources which provide signal information subject to

4 predetermined network distribution security layers; and

5 a security mechanism connected to each of said plurality of receivers, said  
6 security mechanism being configured to remove the network distribution security  
7 layers from the received signals, wherein said plurality of receivers and said security  
8 mechanism are located within a set-top structure.

9  
10 25. A set-top system according to claim 24 wherein said security mechanism is  
11 configured to be renewable and removable from said set-top structure.

12 26. The set-top system according to claim 24 wherein said security mechanism  
13 is a conditional access module which is a removable plug-in type element which is  
14 adapted to be plugged into a cooperating receptacle or socket in a host set-top box.

15 27. The set-top system according to claim 24 wherein the set-top box functions  
16 are located inside a television receiver cabinet which houses a display unit or picture

3 tube.

1 28. The set-top system according to claim 24 wherein said security mechanism  
2 is adapted to plug into a cooperating receptacle.

1 29. A communication system comprising:

2 a plurality of receivers configured for communication with one or more  
3 broadband signal transmission sources producing signals in a selected transport stream  
4 format; and

5 a security mechanism connected to each of said plurality of receivers, said  
6 security mechanism being configured to select one or more of the received signal  
7 transport streams and to remove the network distribution security restrictions  
8 therefrom.

1 30. The communication system according to claim 29 wherein said plurality of  
2 receivers includes an in-band channel and an out-of-band channel, which are adapted  
3 to receive incoming signals from a remote broadcasting station.

1 31. The communication system according to claim 30 wherein said in-band  
2 and out-of-band channels are connected with a filter bank configured to detect

3 predefined digital patterns within received signals and to react thereto for establishing  
4 connections with appropriate ones of predetermined software applications.

1 32. The communication system according to claim 29 further including a smart  
2 card channel configured to enable communications with at least a single applications.

1 33. A digital signal receiving system comprising:  
2 an input signal channel for receiving a digital data stream which carries digital  
3 television signals, wherein the data stream is transmitted in one of a plurality of  
4 different digital transmission formats;  
5 transmission format converter circuitry for converting the incoming data stream  
6 into a transmission format independent set of digital television signals;  
7 and a television display mechanism for converting the transmission format  
8 independent digital television signals into a visual image.

1 34. A digital signal receiving system in accordance with Claim 33 wherein:  
2 the transmission format converter circuitry includes a qualifying mechanism for  
3 receiving and qualifying incoming data bytes according to their positions and values in  
4 their plural-byte data packets;  
5 the transmission format converter circuitry includes a tagging mechanism for

6 assigning a plural-bit tag to each data byte, such tag having a value determined by the  
7 results of the qualifying process performed by the qualifying mechanism;  
8 and the receiving system includes signal processing circuitry responsive to the  
9 tagged data bytes for supplying television signals to the television display mechanism.

1 35. A digital signal receiving system in accordance with Claim 34 wherein the  
2 qualifying mechanism comprises a parser mechanism for analyzing data bytes and  
3 determining their relationships to other data bytes in a plural-byte data packet.

1 36. A digital signal receiving system comprising:  
2 at least two input signal channels for receiving at least two digital data streams,  
3 one of which carries digital television signals and the other of which carries digital  
4 message signals, wherein each data stream is transmitted in one of a plurality of  
5 different transmission formats;  
6 transmission format converter circuitry for converting each incoming data  
7 stream into a common transmission format independent set of signals;  
8 a television display mechanism for converting the transmission format  
9 independent television signals into a visual image;  
10 and a message processing mechanism for converting the transmission format  
11 independent message signals into user perceivable messages.

1           37. A digital signal receiving system in accordance with Claim 36 wherein the  
2        transmission format converter circuitry comprises:

3           a first qualifying mechanism for receiving and qualifying incoming television  
4        signal bytes according to their positions and values in their plural-bit data packets;  
5           a first tagging mechanism for assigning a plural-bit tag to each television signal  
6        byte, such tag having a value determined by the results of the qualifying process  
7        performed by the first qualifying mechanism;

8           first signal processing circuitry responsive to the tagged television signal bytes  
9        for supplying television signals to the television display mechanism;

10          a second qualifying mechanism for receiving and qualifying incoming message  
11        signal bytes according to their positions and values in their plural-bit data packets;

12          a second tagging mechanism for assigning a plural-bit tag to each message  
13        signal byte, such tag having a value determined by the results of the qualifying process  
14        performed by the second qualifying mechanism;

15          and second signal processing circuitry responsive to the tagged message signal  
16        bytes for supplying message signals to the message processing mechanism.

1           38. A digital signal receiving system in accordance with Claim 37 wherein  
2        each qualifying mechanism comprises a parser mechanism for analyzing data bytes

3 and determining their relationships to other data bytes in a plural-byte data packet.

1           39. A digital signal receiving system for receiving a plurality of different  
2 digital data transport stream formats, such system comprising:

3           a qualifying mechanism for receiving and qualifying incoming data bytes  
4 according to their positions and values in their plural-byte data packets;

5           a tagging mechanism for assigning a plural-bit tag to each data byte, such tag  
6 having a value determined by the results of the qualifying process performed by the  
7 qualifying mechanism;

8           and a signal processing mechanism responsive to the tagged data bytes for  
9 producing digital information signals.

1           40. A multiple data transport mechanism for receiving a plurality of different  
2 digital data transport stream formats, such mechanism comprising:

3           a qualifying mechanism for receiving and qualifying incoming data bytes  
4 according to their positions and values in their plural-byte data packets;

5           and a tagging mechanism for assigning a plural-bit tag to each data byte, such  
6 tag having a value determined by the results of the qualifying process performed by  
7 the qualifying mechanism.

1           41. A multiple data transport mechanism in accordance with Claim 40  
2        wherein the qualifying mechanism comprises a parser mechanism for analyzing data  
3        bytes and determining their relationships to other data bytes in a multi-byte data  
4        packet.

1           42. A multiple data transport mechanism for receiving a plurality of different  
2        digital data transport stream formats wherein data is conveyed in multi-byte data  
3        packets with each packet having a plural-byte header field and a plural-byte payload  
4        field, such mechanism comprising:

5               a first testing mechanism for examining each incoming data byte and  
6        determining whether the byte is a header byte or a payload byte;

7               a first tagging mechanism coupled to the first testing mechanism for assigning  
8        header byte indicative tags to header field data bytes and payload indicative tags to  
9        payload field data bytes;

10              a second testing mechanism for examining each incoming data byte and  
11        determining whether the data is scrambled;

12              a second tagging mechanism coupled to the second testing mechanism for  
13        assigning a scramble condition tag bit to each data byte and giving such bit one binary  
14        value if the data is scrambled and the other binary value if the data is not scrambled;  
15              and signal transfer circuitry for transferring each data byte and its assigned tag

16 bits to a data processing mechanism for producing usable digital information.

## **ABSTRACT OF THE DISCLOSURE**

Conditional access methods and apparatus are provided for use with digital television receivers and other digital broadband receivers. The methods and apparatus are capable of handling several different digital signal transmission protocols in an automatic and flexible manner. An input unit is provided for analyzing and tagging incoming data bytes so that further processing operations are less dependent on the transmission format being received. A cipher handling unit is provided for adapting in real time the scrambling and descrambling performances to match the requirements of the transmission network and the receiving apparatus. A filtering mechanism is provided for filtering and handling multiple asynchronous data streams in a parallel manner.

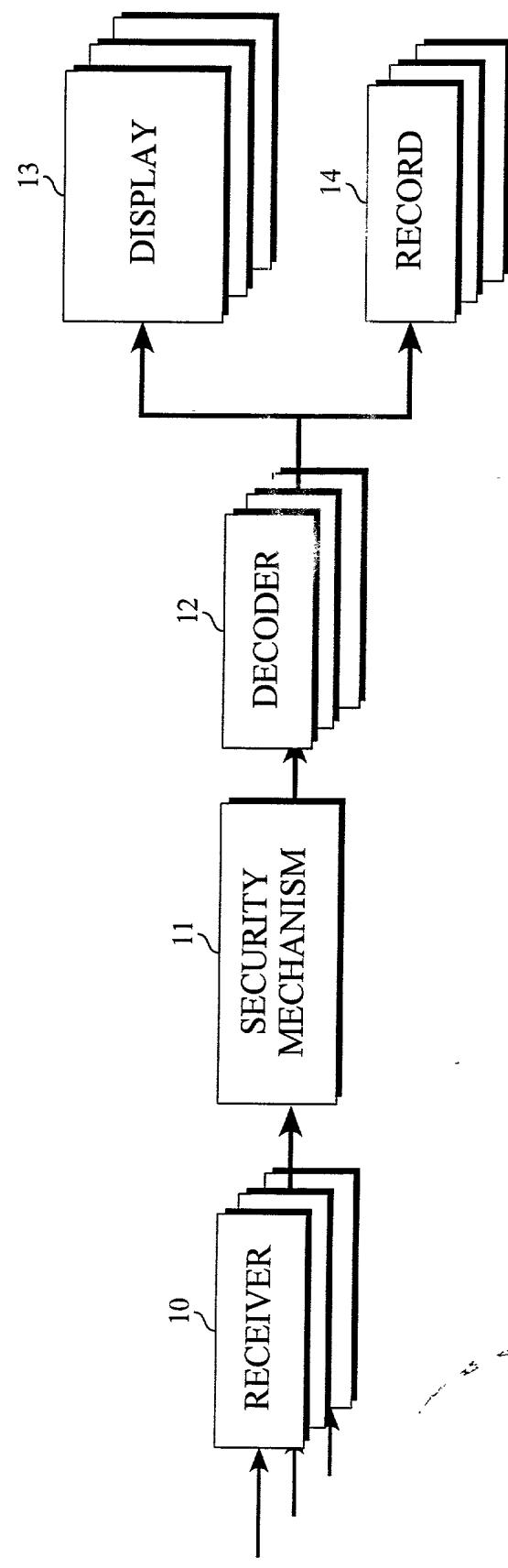
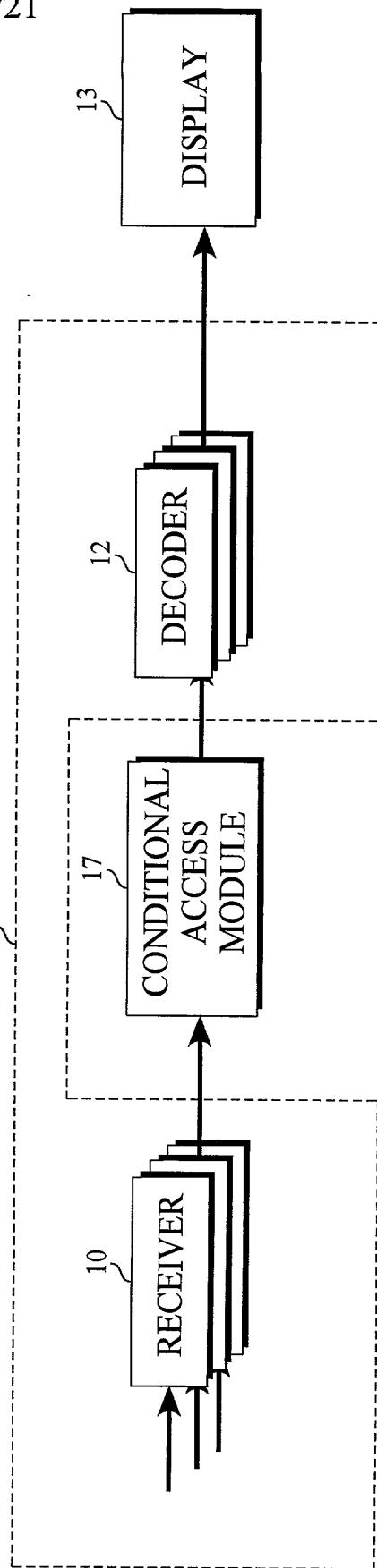
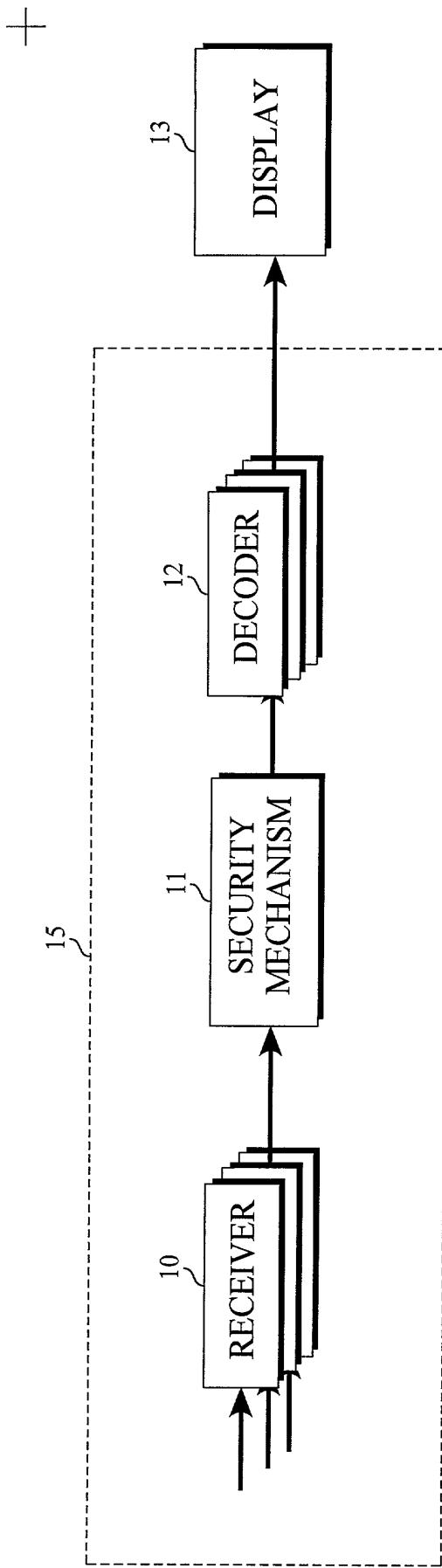


Fig. 1



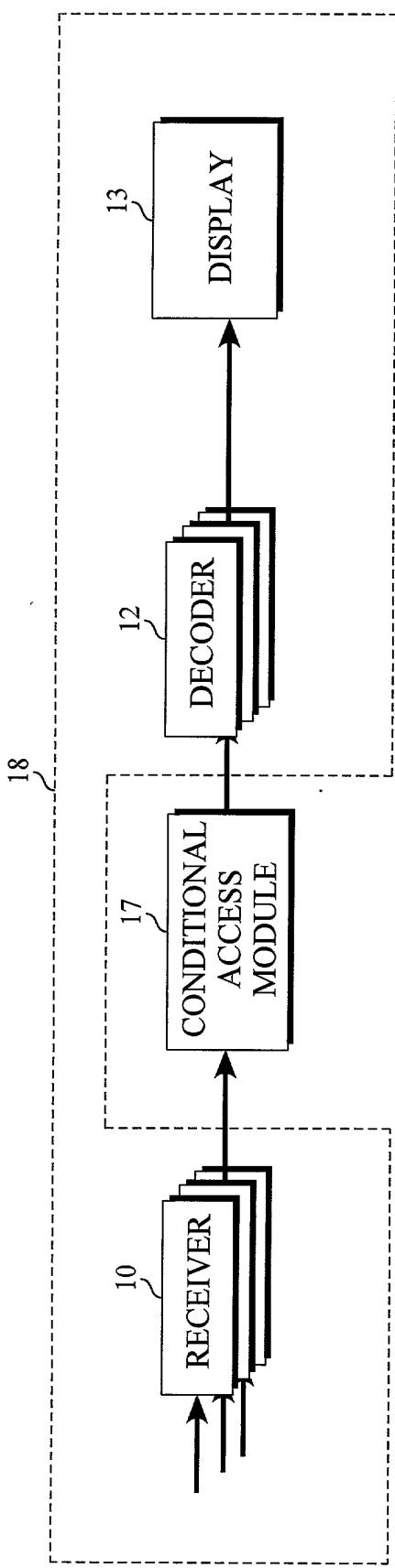


Fig. 26

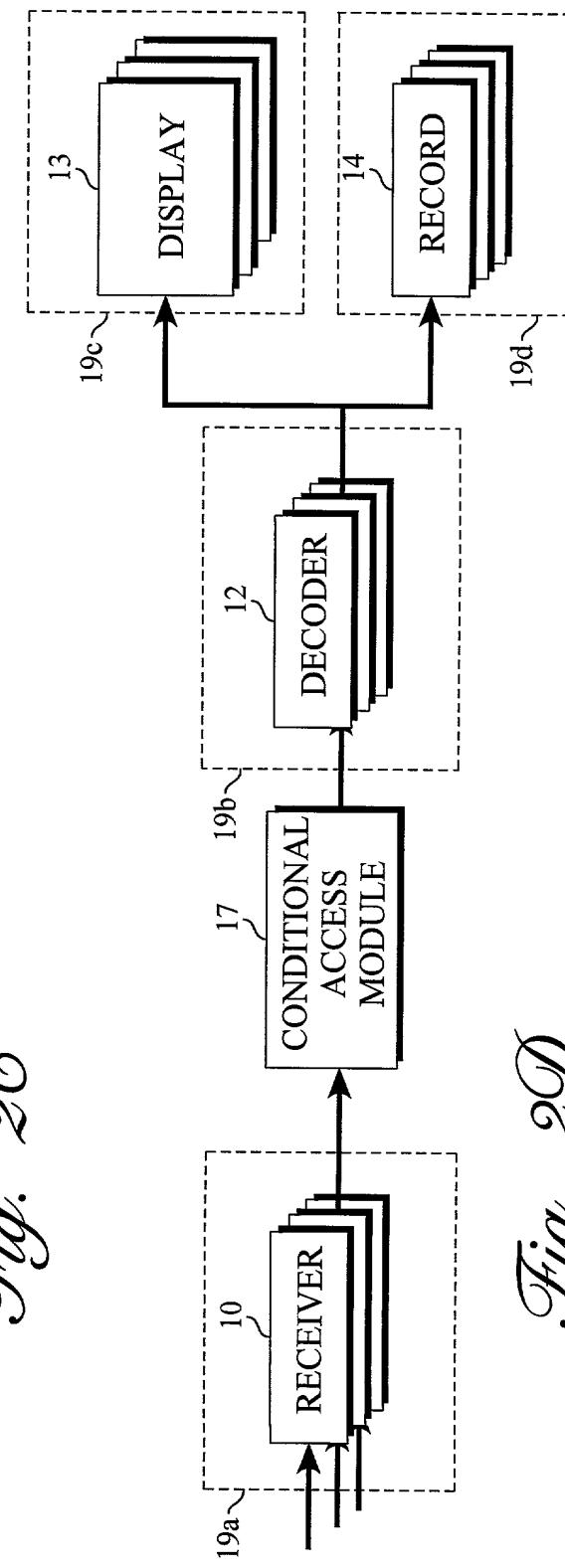
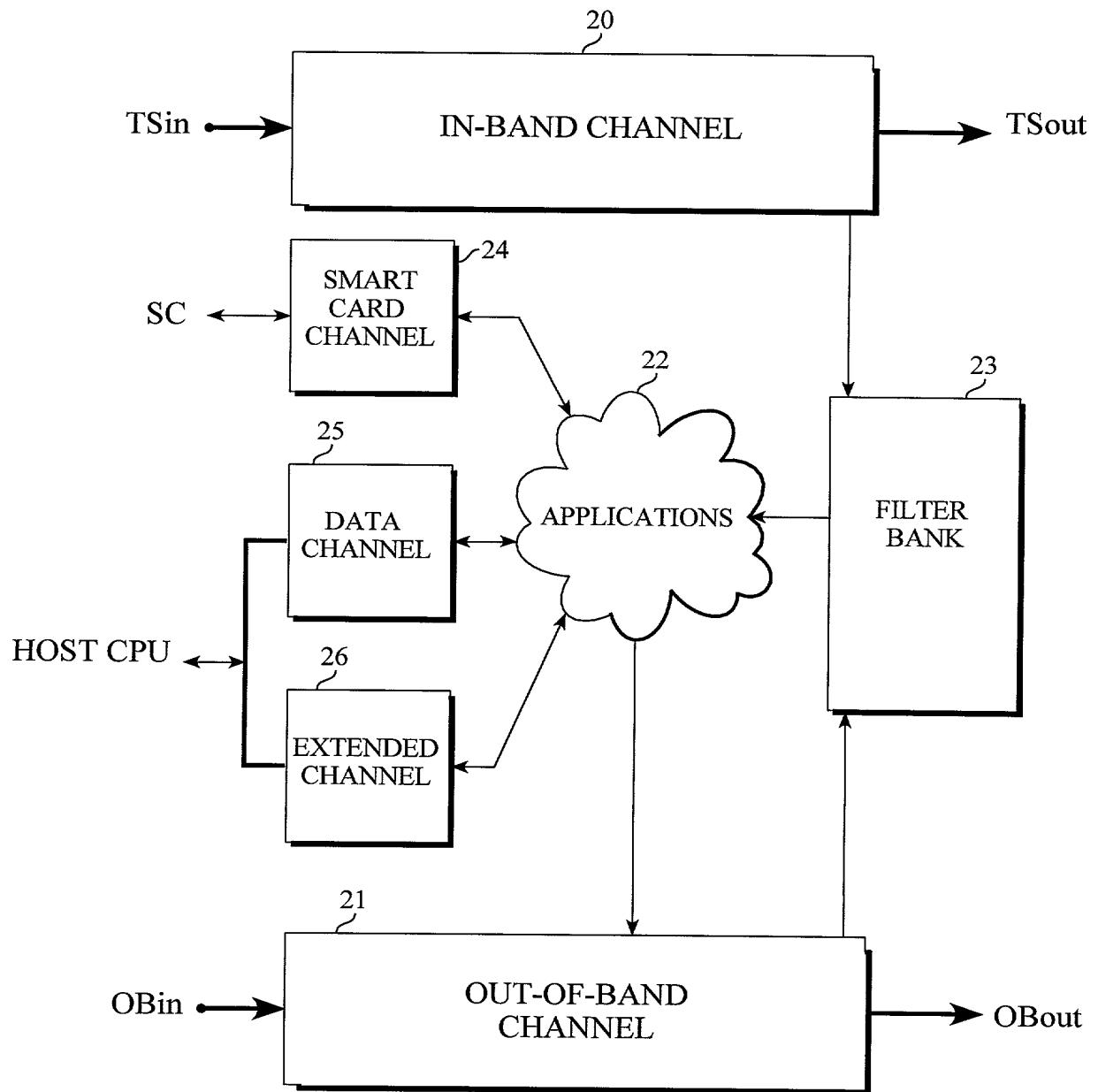


Fig. 2D



*Fig. 3*

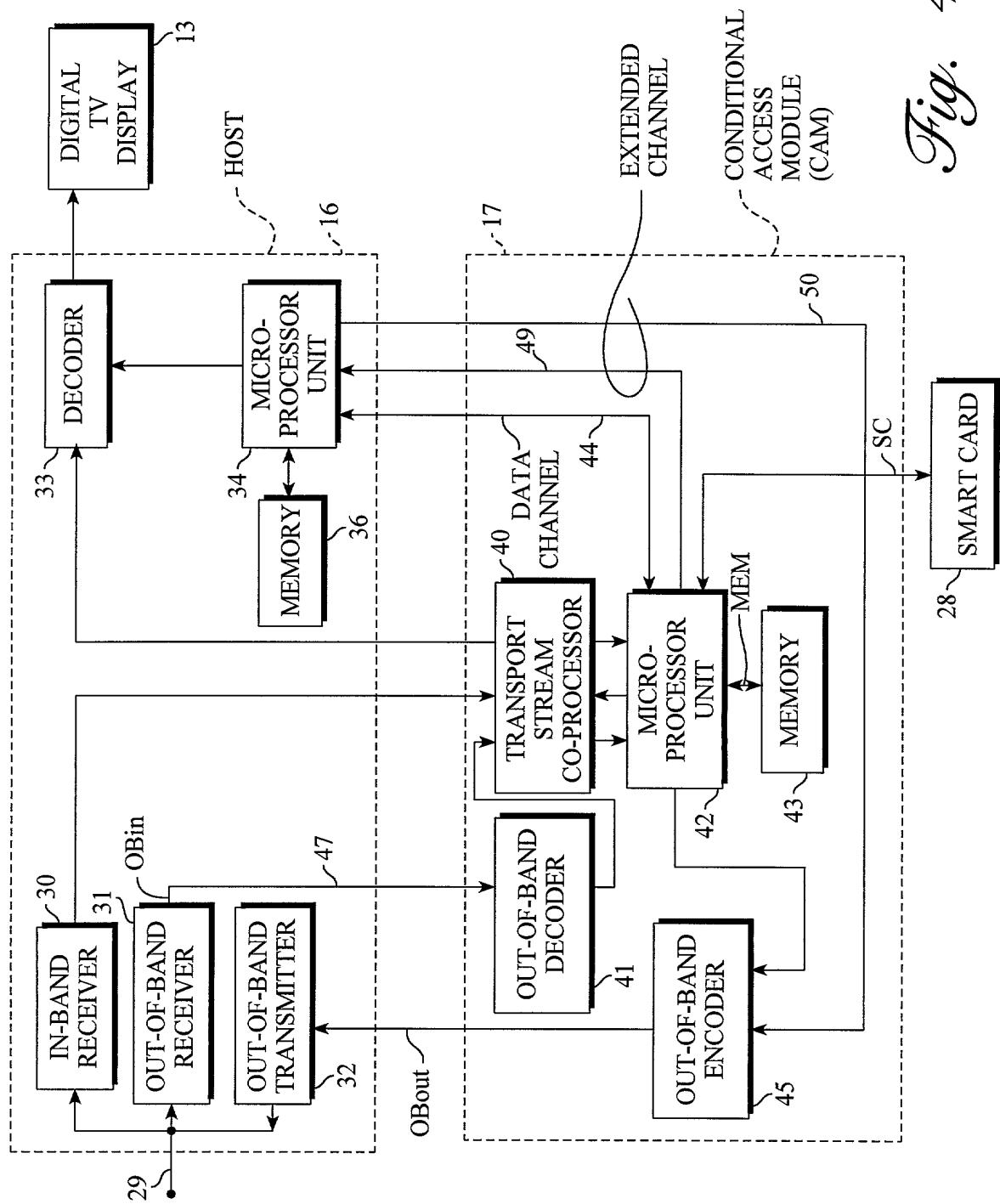


Fig. 4

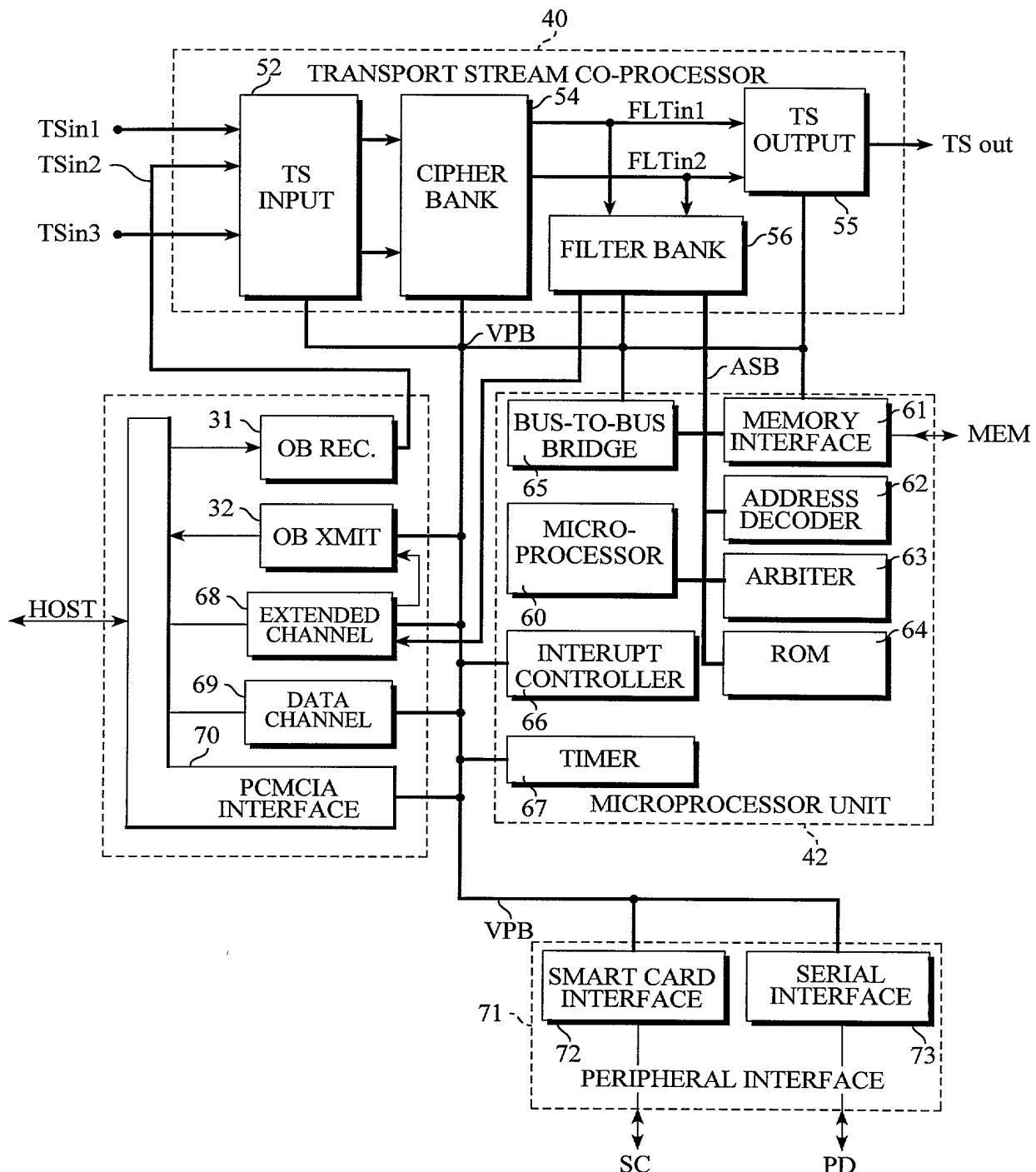


Fig. 5

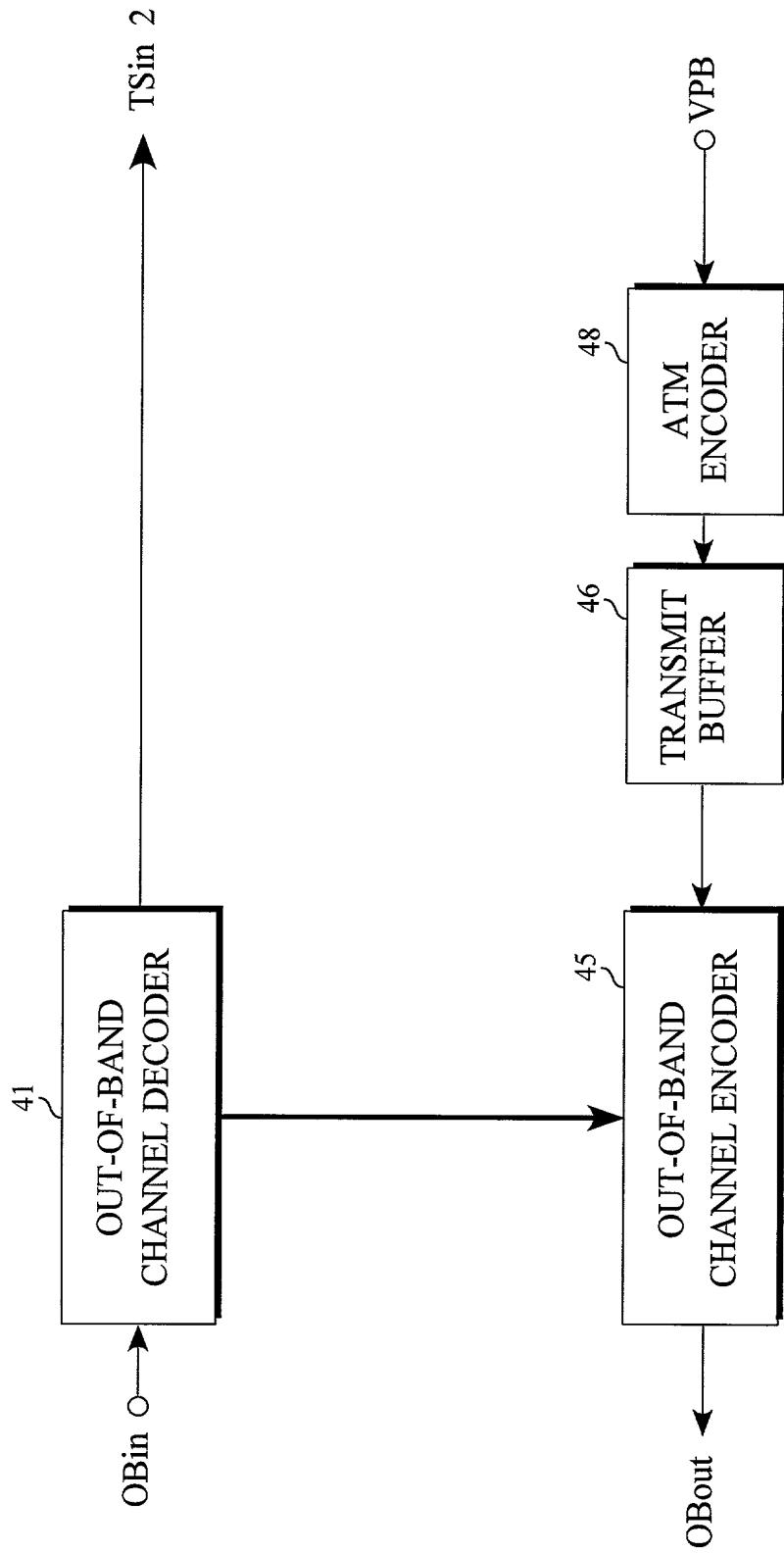


Fig. 6

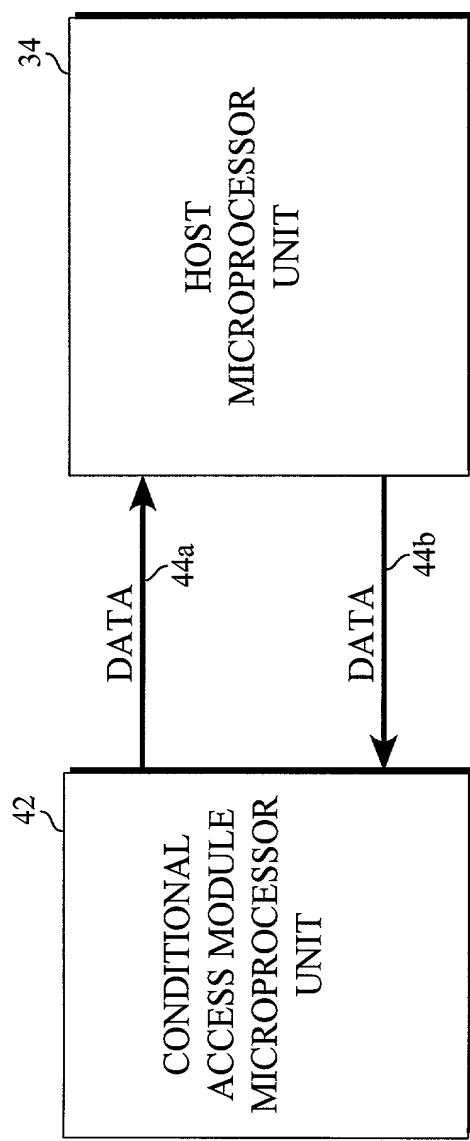


Fig. 7

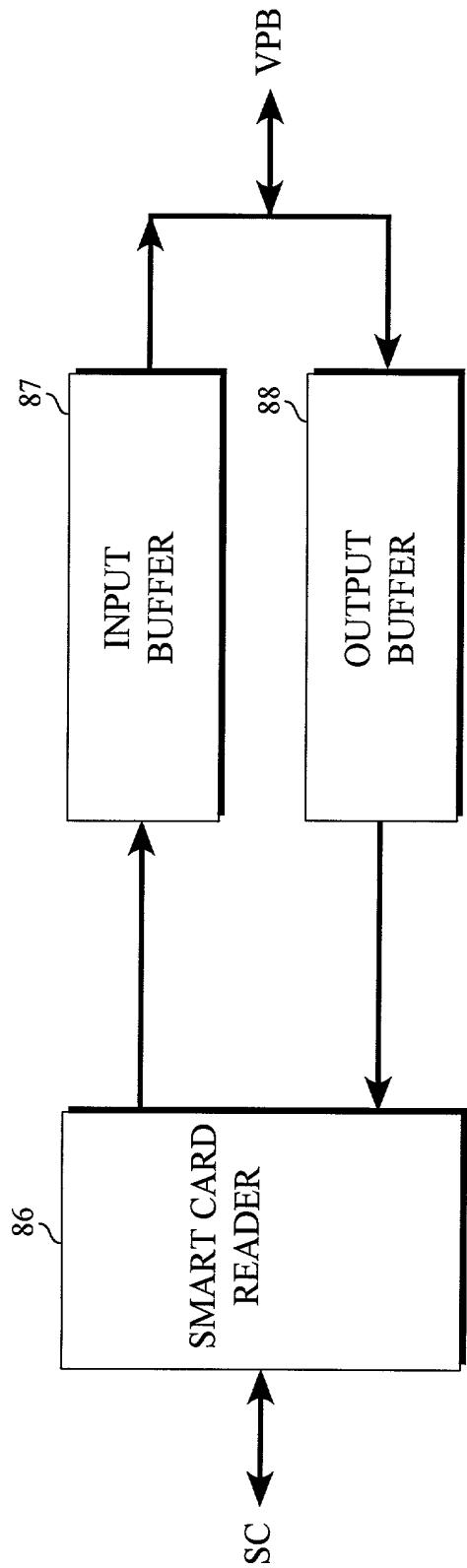


Fig. 8

+

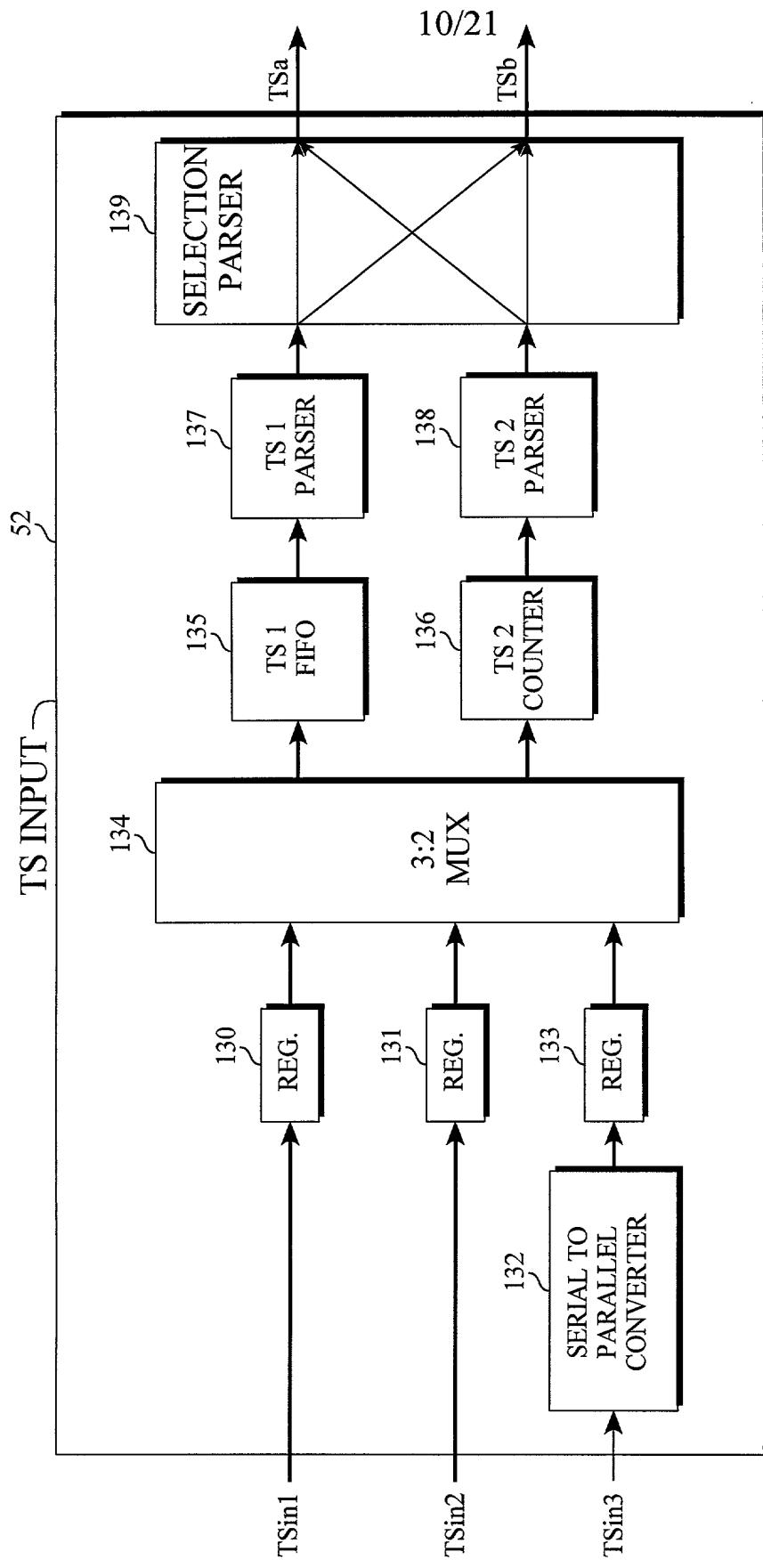


Fig. 9

+

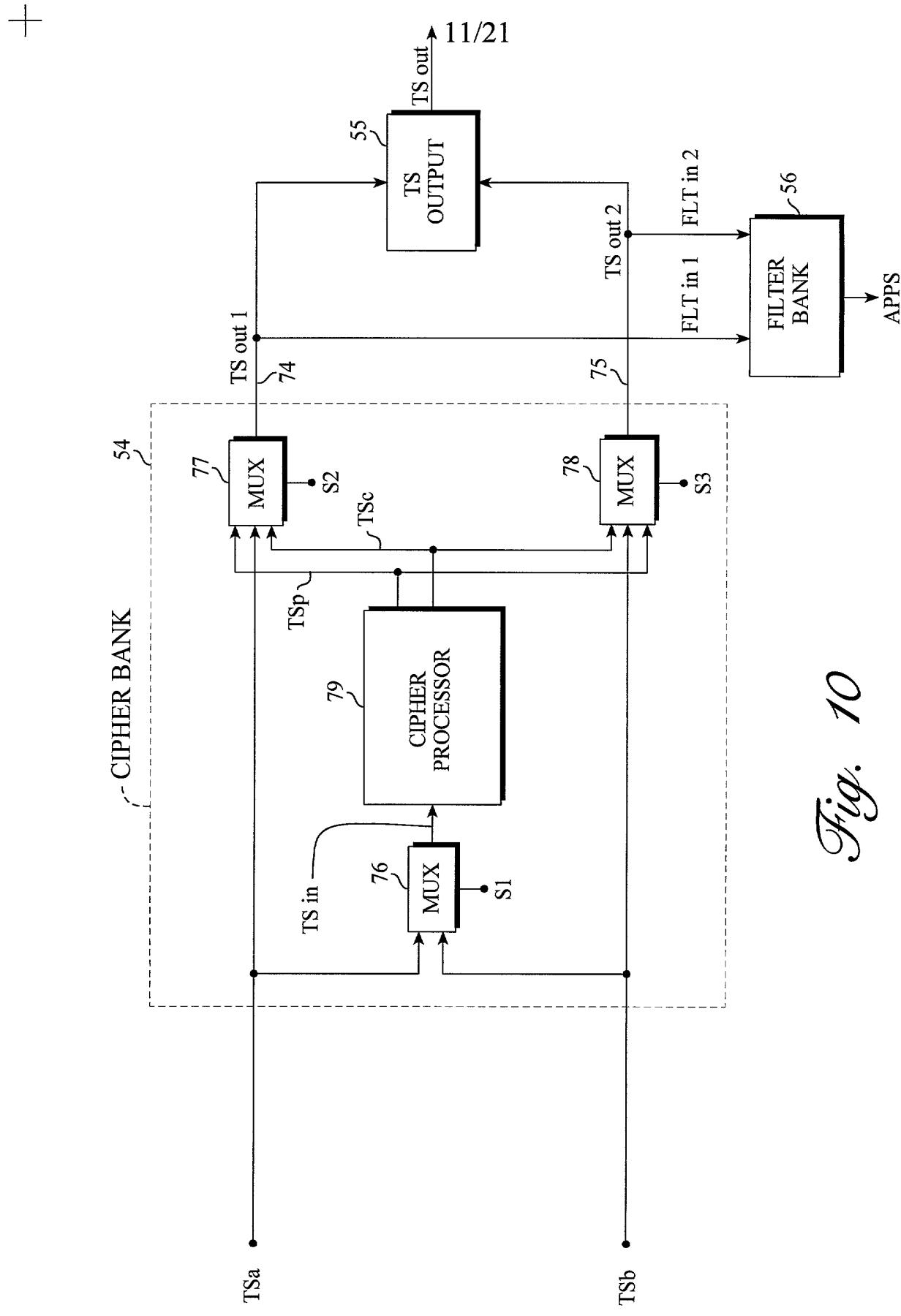


Fig. 10

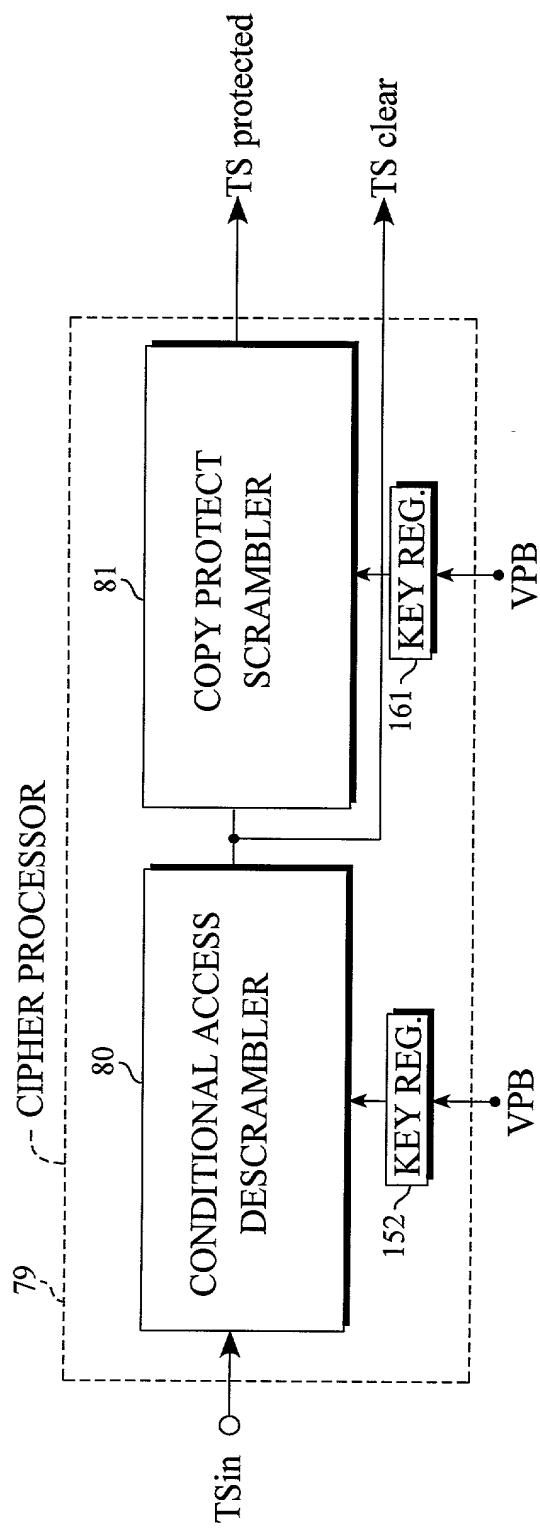


Fig. 11

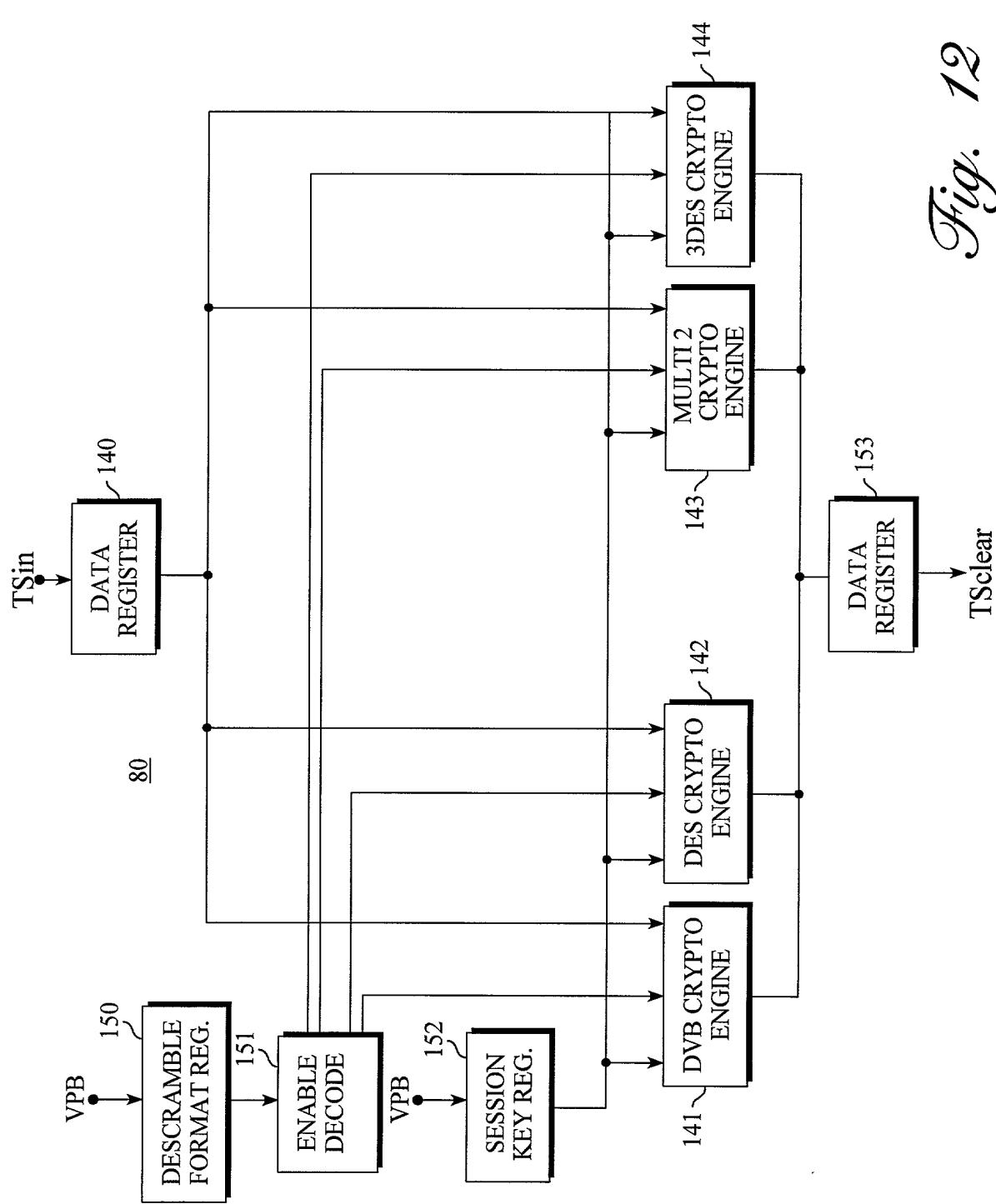
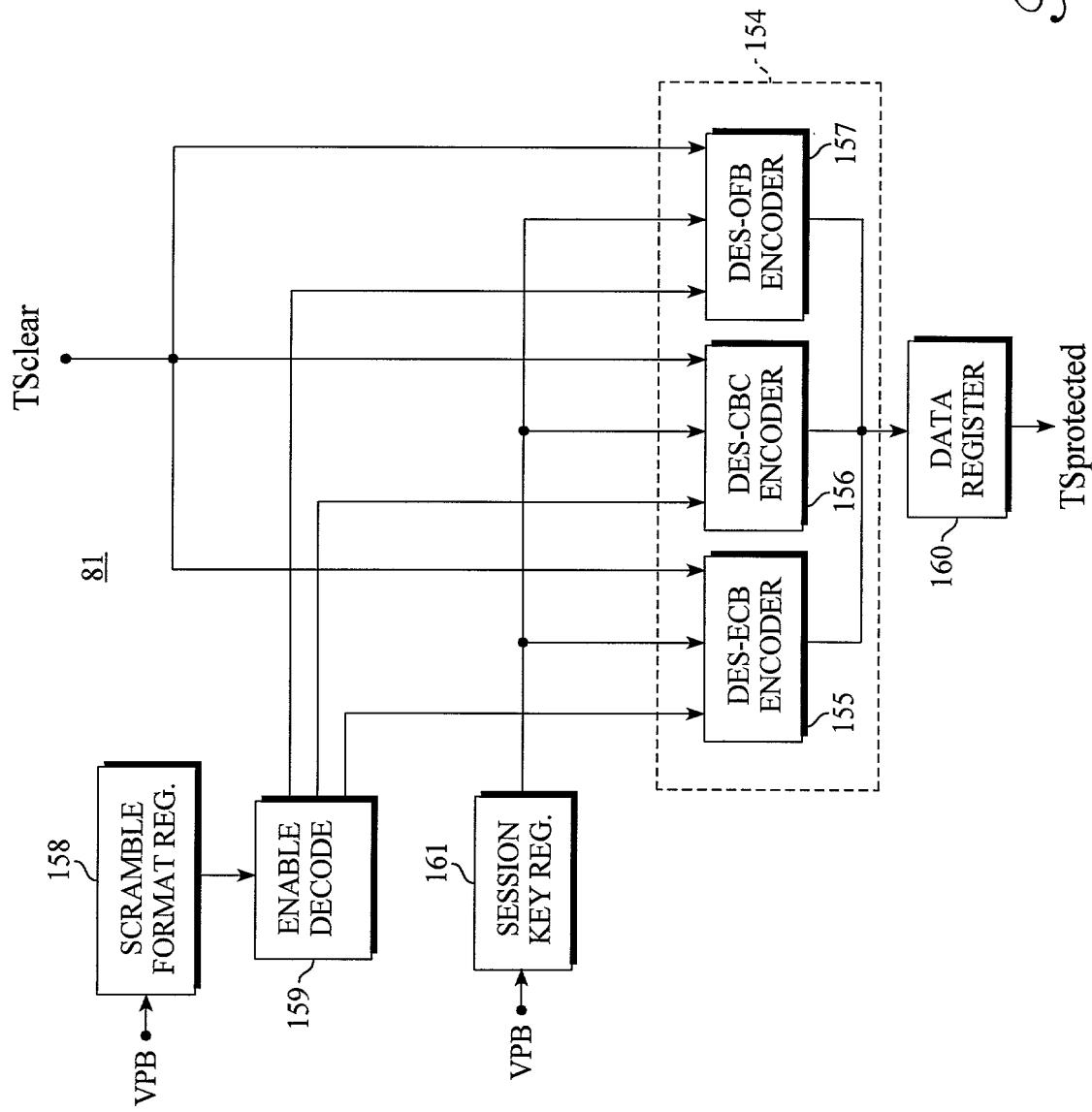


Fig. 12



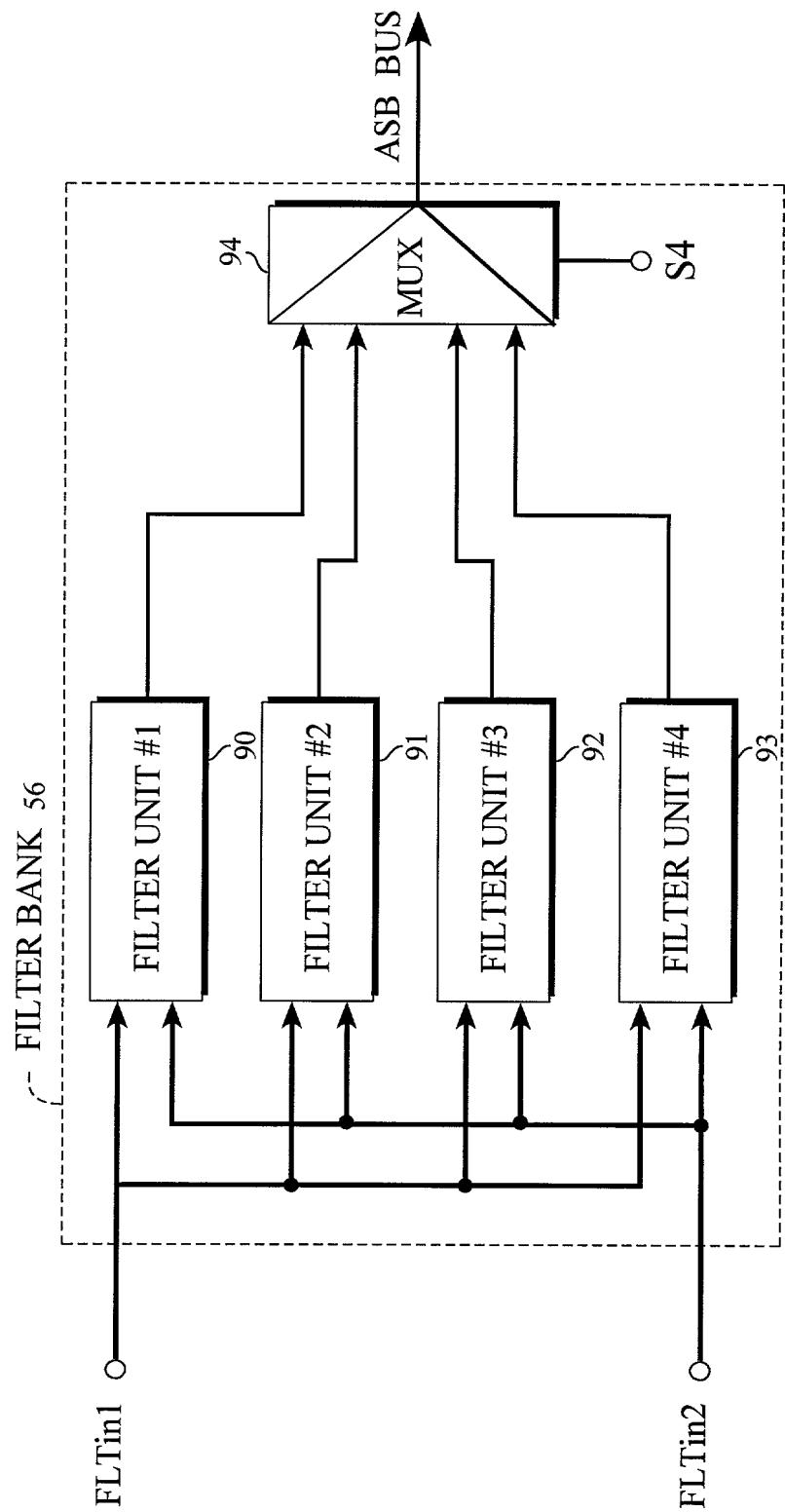


Fig. 14

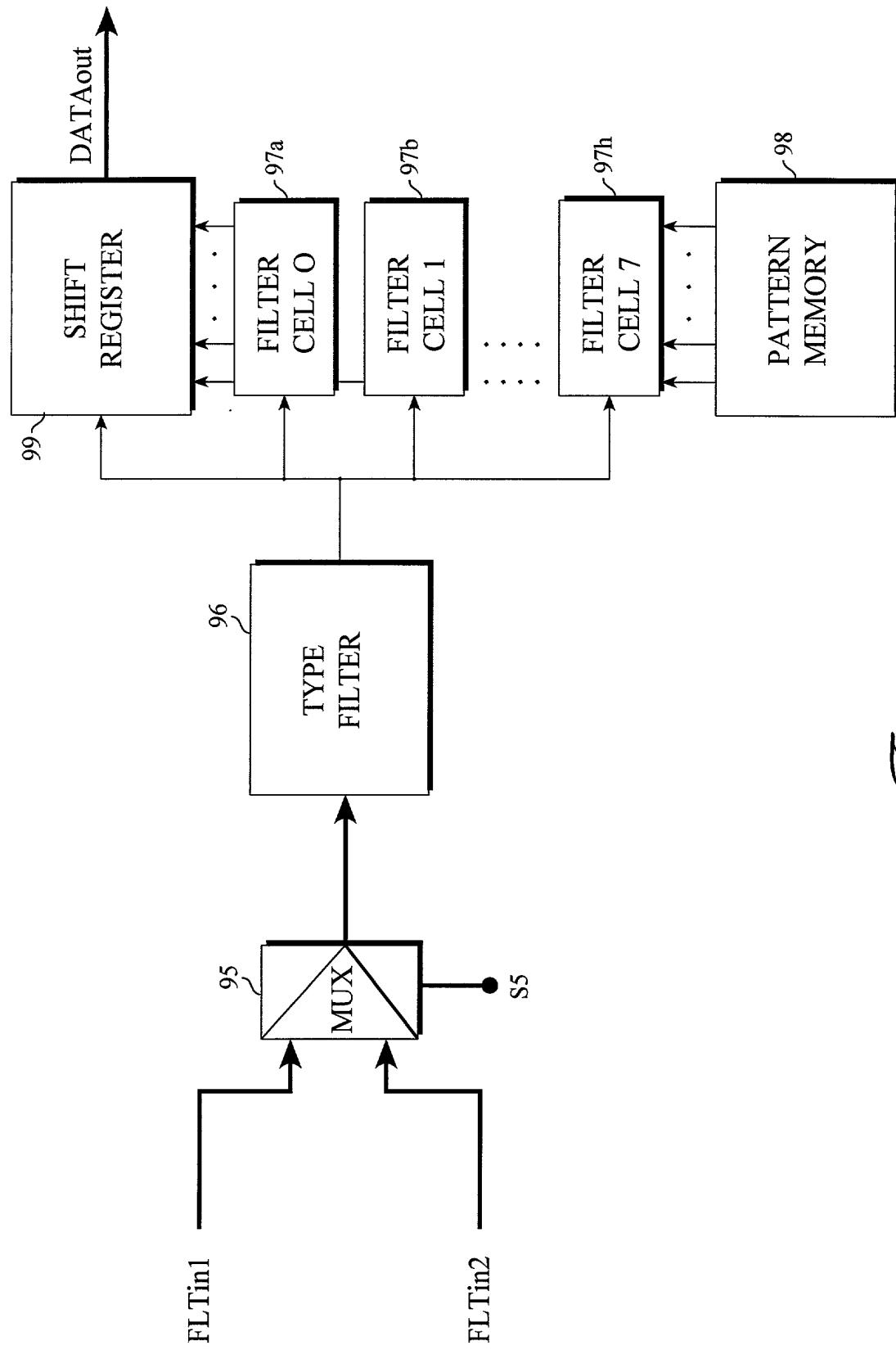


Fig. 15

+

+

Fig. 16B

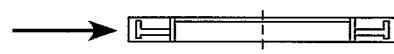


Fig. 16

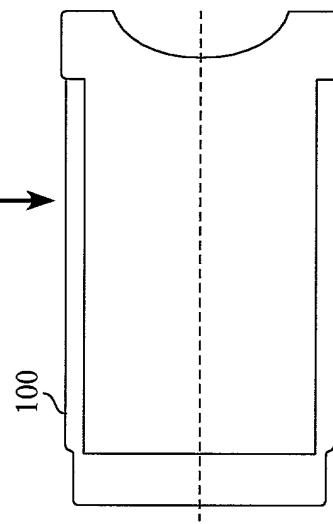
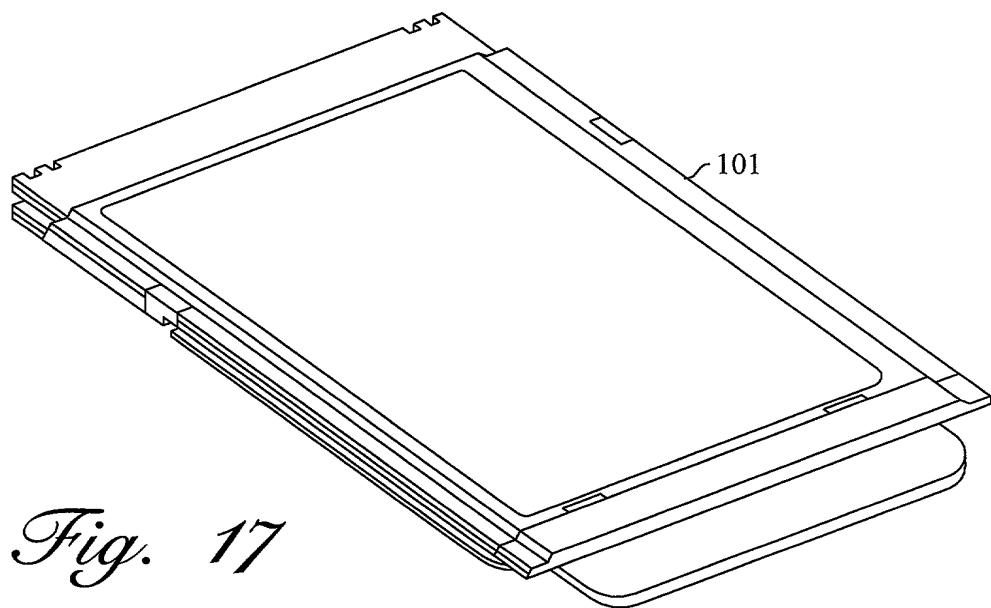


Fig. 16A

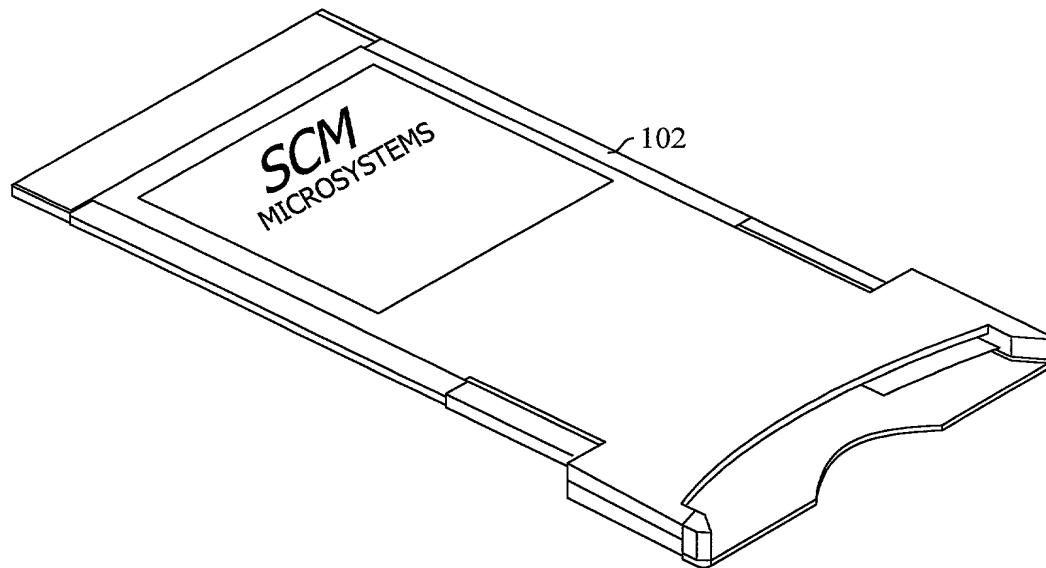


Fig. 16C





*Fig. 17*



*Fig. 18*

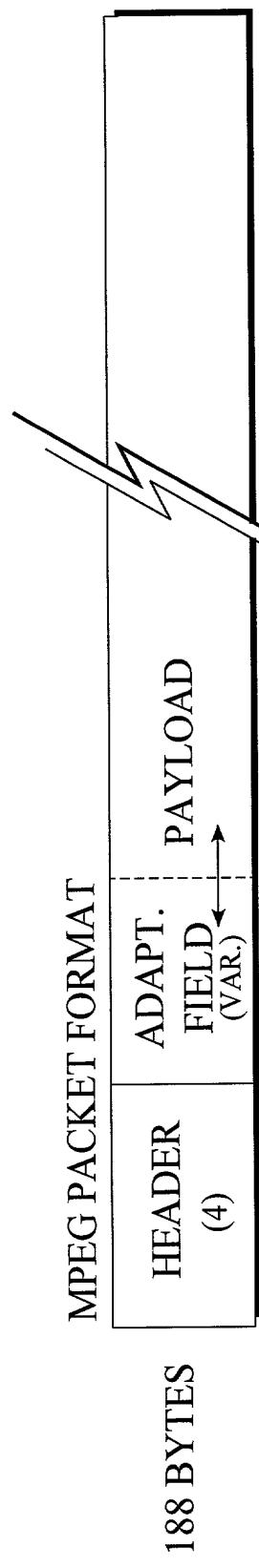


Fig. 19

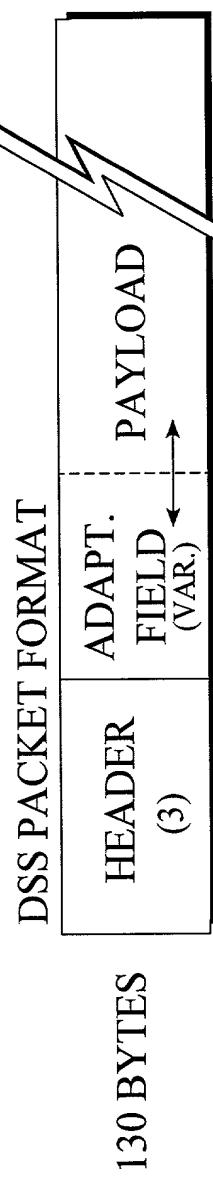


Fig. 20

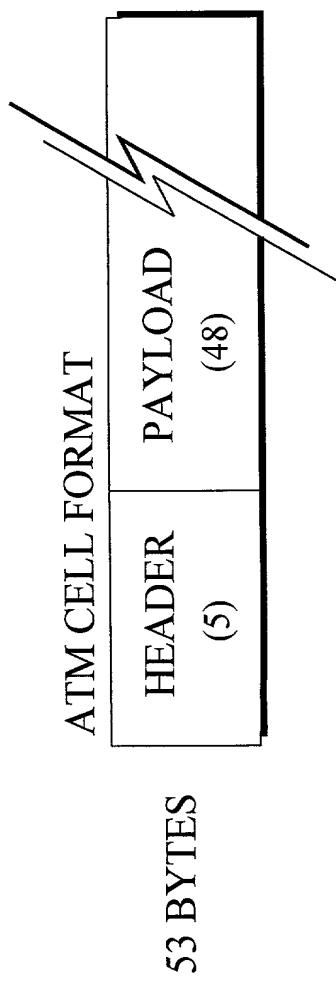
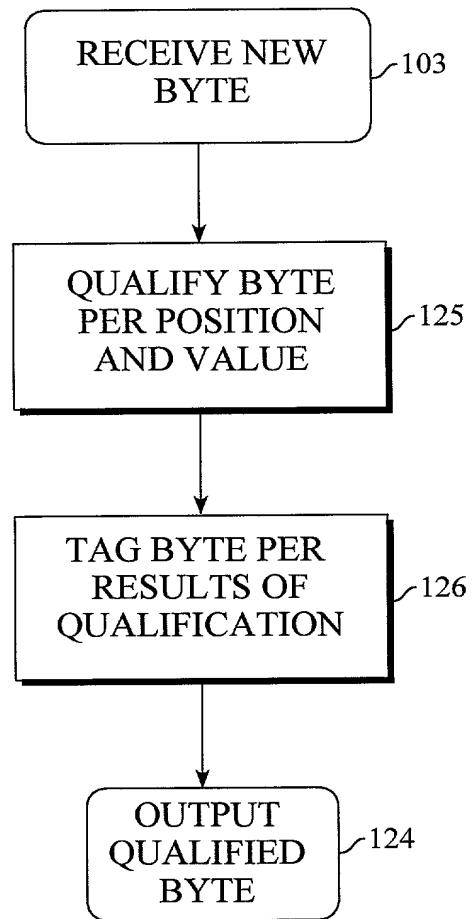


Fig. 21



*Fig. 22*

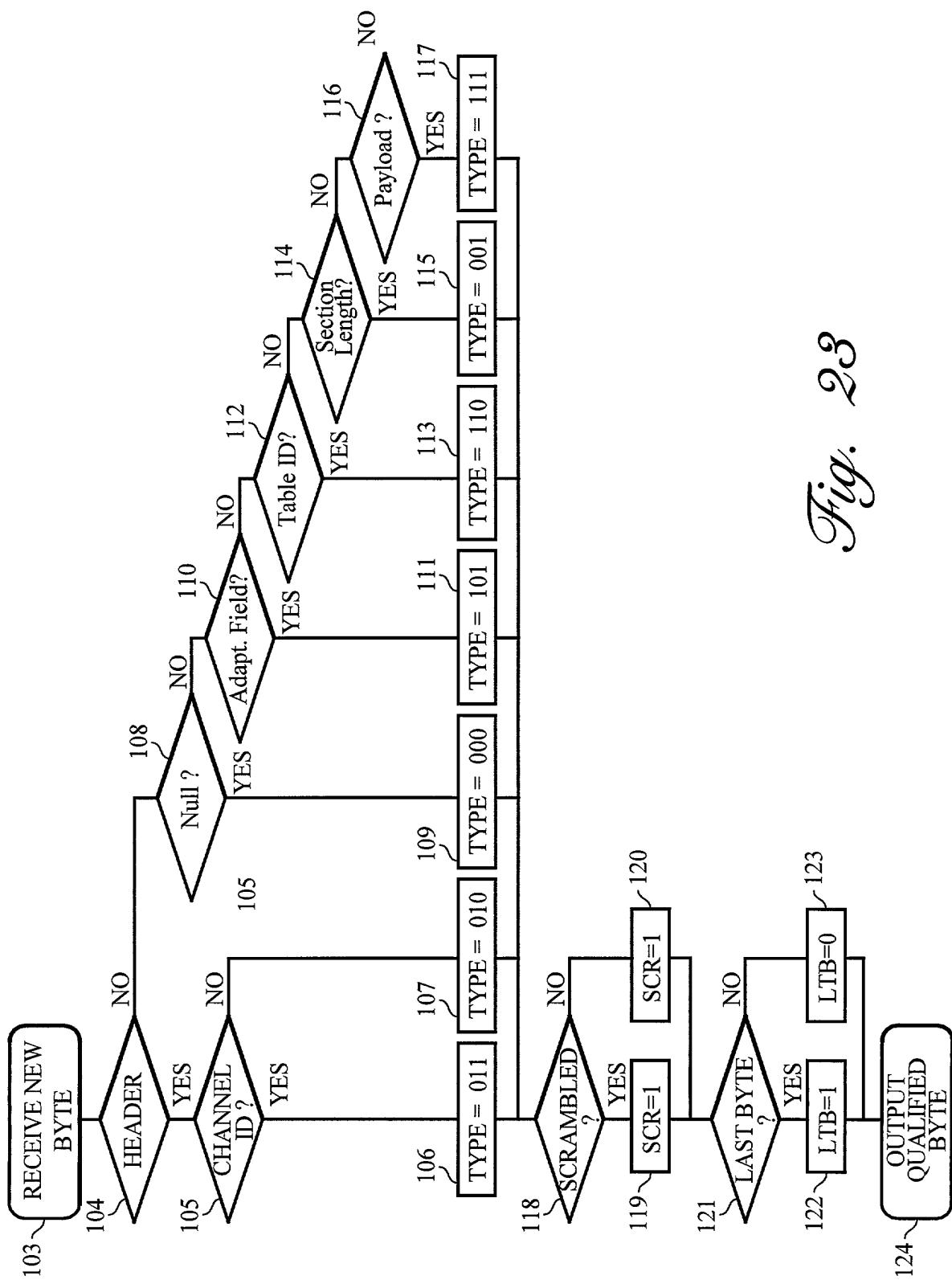


Fig. 23

**DECLARATION AND POWER OF ATTORNEY**  
**Original Application**

As below named inventors, we declare that we have reviewed and understand the contents of the specification, including the claims, as amended by any amendment specifically referred to in this Declaration, that the information given herein is true, that we believe that we are the original, first and joint inventors of the invention entitled:

**DIGITAL TELEVISION CONDITIONAL ACCESS METHODS AND APPARATUS WITH  
MULTIPLE DATA TRANSPORT MECHANISM**

which is described and claimed in:

the attached specification or  
 the specification in application Serial No. \_\_\_\_\_ filed \_\_\_\_\_.  
 The present application is a continuation-in-part of Prior Application Serial No. \_\_\_\_\_ filed \_\_\_\_\_ and may be considered to disclose and claim subject matter in addition to that disclosed in the Prior Application, and I hereby claim the benefit of 35 U.S.C. Section 120.

that we acknowledge our duty to disclose information in accordance with 37 C.F.R. Section 1.56 and defined on the attached sheet, which is material to the examination of this application, that we do not know and do not believe the same was ever known or used in the United States of America before my or our invention thereof, or more than one year prior to this application, or in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application and that as to applications for patent or inventor's certificate filed by me or my legal representatives or assigns in any country foreign to the United States of America, the earliest filed foreign application(s) filed within twelve months prior to the filing date of this application and all foreign applications filed more than twelve months prior to the filing date of this application, if any, are identified below.

**CHECK APPROPRIATE BOX**

No earlier-filed foreign applications.  
 Requirement information as to foreign applications filed prior to filing date of this application is on page \_\_\_\_\_ attached hereto and made a part hereof.

**POWER OF ATTORNEY:**

As named inventors, we hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

<u>NAME</u>	<u>REGISTRATION NO.</u>
Robert P. Sabath	29,107
Bobby K. Truong	37,499
John F. Schipper	26,994
Stanley N. Protigal	28,657
Richard E. Bee	18,005
George M. Steres	36,690
of SABATH & TRUONG	

**SEND CORRESPONDENCE TO**

**SABATH & TRUONG**  
111 N. Market Street, Suite 815  
San Jose, California 95113

**DIRECT TELEPHONE CALLS TO**

Tel: 408/293-9934  
Fax: 408/293-2183

FULL NAME OF INVENTOR 1	LAST NAME <b>VANTALON</b>	FIRST NAME <b>LUC</b>	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY <b>SUNNYVALE</b>	STATE OR FOREIGN COUNTRY <b>CALIFORNIA</b>	COUNTRY OF CITIZENSHIP <b>FRANCE</b>	
POST OFFICE ADDRESS	POST OFFICE ADDRESS <b>1396 CORDILLERAS AVE.</b>	CITY <b>SUNNYVALE</b>	STATE OR COUNTRY <b>USA</b>	ZIP CODE <b>95087</b>
FULL NAME OF INVENTOR 2	LAST NAME <b>CHATAIGNIER</b>	FIRST NAME <b>ARNAUD</b>	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY <b>F-13600 CEYRESTE</b>	STATE OR FOREIGN COUNTRY <b>FRANCE</b>	COUNTRY OF CITIZENSHIP <b>FRANCE</b>	
POST OFFICE ADDRESS	POST OFFICE ADDRESS <b>31 allée de la Granette</b>	CITY <b>F-13600 CEYRESTE</b>	STATE OR COUNTRY <b>FRANCE</b>	ZIP CODE
FULL NAME OF INVENTOR 3	LAST NAME <b>GENEVOIS</b>	FIRST NAME <b>CHRISTOPHE</b>	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY <b>13600 LA CIOTAT</b>	STATE OR FOREIGN COUNTRY <b>FRANCE</b>	COUNTRY OF CITIZENSHIP <b>FRANCE</b>	
POST OFFICE ADDRESS	POST OFFICE ADDRESS <b>47, Avenue de la Paix</b>	CITY <b>13600 LA CIOTAT</b>	STATE OR COUNTRY <b>FRANCE</b>	ZIP CODE

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

NAME	SIGNATURE	DATE
LUC VANTALON		
NAME	SIGNATURE	DATE
ARNAUD CHATAIGNIER		
NAME	SIGNATURE	DATE
CHRISTOPHE GENEVOIS		

Section 1.56 Duty to Disclose Information Material to Patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by Sections 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applications to carefully examine:

(1) prior art cited in search report of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the application takes in:

(i) opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any considerations given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent or inventor.